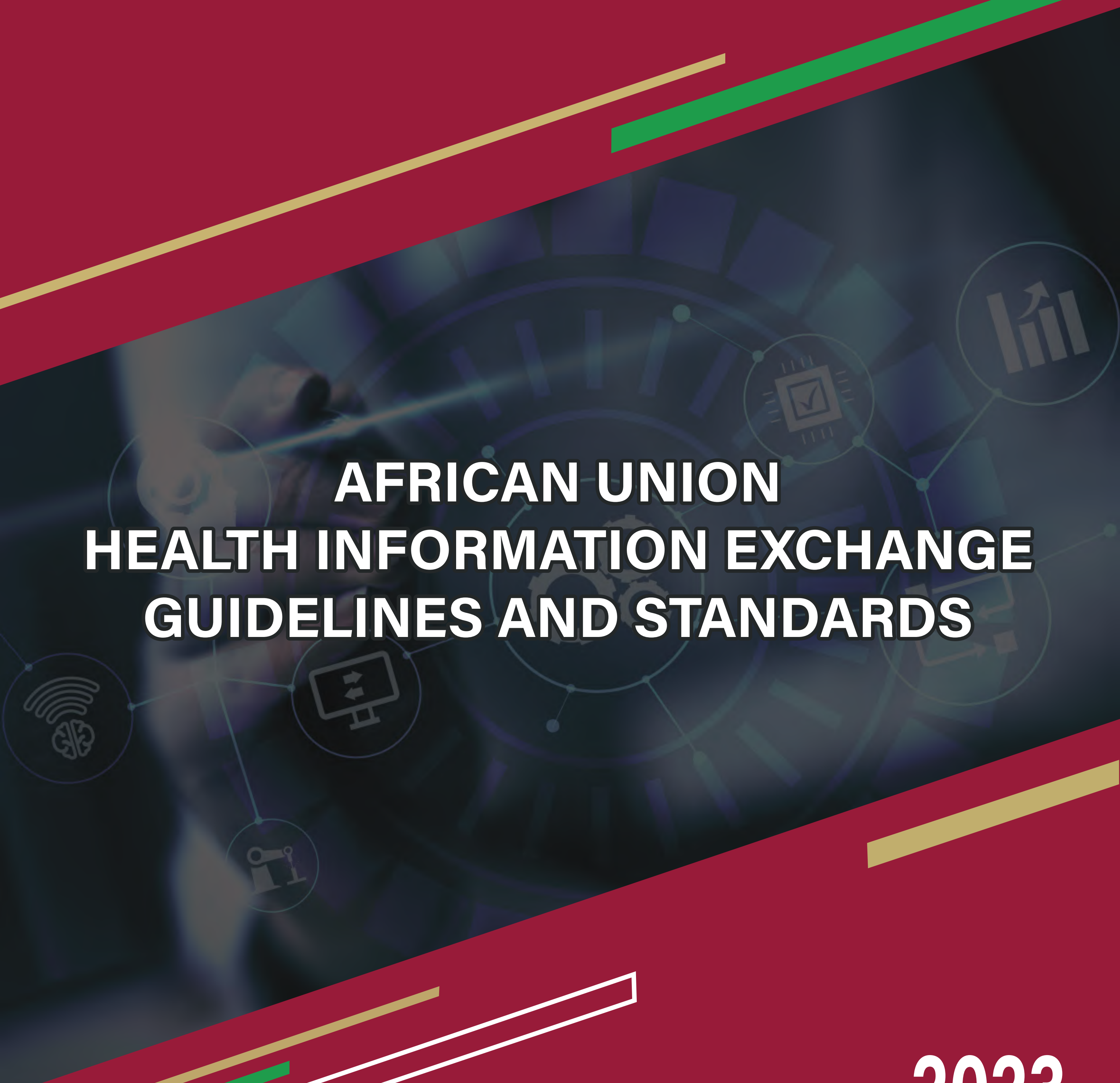
African Union

AFRICA CDC
Centres for Disease Control and Prevention
Safeguarding Africa's Health



AFRICAN UNION HEALTH INFORMATION EXCHANGE GUIDELINES AND STANDARDS

2023

+251 11 551 77 00 africacdc@africa-union.org africacdc@africa-union.org

Table of Contents

Acronyms

ADX	Aggregate Data Exchange
ADT	Admit Discharge Transfer
AIDS	Acquired Immunodeficiency Syndrome
APPC	Advanced Patient Privacy Consents
ART	Antiretroviral Therapy
ASCII	American Standard Code for Information Interchange
ASTM	American Society of Testing and Materials
AUDA	African Union Development Agency
AU	African Union
CCD	Continuity of Care Document
CDC	Centers for Disease Control and Prevention
CDA	Clinical Document Architecture
COVID-19	Coronavirus Disease 2019
DHIS2	District Health Information Software Version 2
DICOM	Digital Imaging and Communications in Medicine
DUA	Data Use Agreement
ECA	Economic Commission for Africa
EMR	Electronic Medical Record
EU	European Union
FHIR	Fast Healthcare Interoperability Resources
FTP	File Transfer Protocols
HER	Electronic Health Record
HIS	Health Information System

HISP	Health Information Systems Program
HIE	Health Information Exchange
HL7	Health Level Seven
HIV	Human Immunodeficiency Virus
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAES	Institute of Advanced Engineering and Science
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IHR	International Health Regulations
IPS	International Patient Summary
ICT	Information Communication Technology
ICD	International Classification of Diseases
IDSR	Integrated Disease Surveillance and Response
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LIMS	Laboratory Information Management System
LIS	Laboratory Information System
LOINC	Logical Observation Identifiers Names and Codes
NEPAD	New Partnership for Africa's Development
NIST	National Institute of Standards and Technology

NPHI	National Public Health Institutes
PHI	Public Health Institutes
PHS	Public Health Surveillance
PII	Personally Identifiable Information
POPIA	Protection of Personal Information Act
RCC	Regional Collaborating Centers
REC	Regional Economic Communities
SDG	Sustainable Development Goals
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNOMED-CT	Systematized Nomenclature of Medicine - Clinical Terminology
SOAP	Simple Object Access Protocol
TB	Tuberculosis
TLS	Transport Layer Security
TS	Technical Specification
TS	Technical Specification
TB	Tuberculosis
UN	United Nations
UDP	User Datagram Protocol
WHATWG	Web Hypertext Application Technology Working Group
WHO	World Health Organization
W3C	World Wide Web Consortium
XML	Extensible Markup Language
XUA	User Assertion Profile

Acknowledgments

The Health Information Exchange Task Force team, which was organized by Africa CDC with support from technical experts at the University of Gondar and HISP South Africa, was responsible for the development of this document. We would like to extend our deepest gratitude to each and every member of the task force, as well as the chairpersons, co-chairpersons, reviewers, and all other experts who made significant contributions to the creation of this document. A list of the members of the task force as well as contributors could be seen in Annexure 14.

Preface

The application of digital health technology is growing at a rapid rate in Africa, with the goals of improving the delivery of healthcare services and more effectively reaching out to remote and underserved communities. The lack of enabling guidelines and standards across the continent, on the other hand, makes it difficult to share data in a meaningful way across the continent. Considering this, Africa Centres for Disease Control and Prevention (Africa CDC) established a task force of 24 members to provide expertise and guidance in the development of AU HIE guidelines and standards. Members of the task force were subject matter experts working in Africa and internationally on the collection, analysis, and exchange of health information. Some of these experts had been involved in previous consultations on defining Africa CDC's health information systems strategy. A chairperson, co-chairperson, and secretary were elected to engage the task force members in different technical working groups.

A chairperson, co-chairperson, and secretary were elected to engage the task force members. Three technical working groups were constituted to lead the drafting of the three sections of the document:

1. HIE Policy directions
2. HIE Standards
3. Implementation Use Cases

Following several virtual meetings and consultations, a draft document on AU HIE guidelines and standards was developed. The methodology employed involved the reviewing of scientific publications and governmental reports on HIE guidelines and standards in Africa; reviewing Internationally known comprehensive and robust data exchange standards; and incorporating recommendations from the Africa CDC HIE Task Force Members.

Additionally, the document was critically reviewed and validated by Member States in all AU regions through several validation workshops; West Africa (validation workshop took place in Senegal), Central Africa (Congo-Brazaville), East Africa (Rwanda), South Africa (Namibia) and North Africa (Mauritania) through validation workshops. Representatives of Africa CDC, Regional

Collaborating Centres (RCC), World Health Organization (WHO), West African Health Organization (WAHO), East, Central and Southern Africa Health Community (ECSA), and Economic Community of Central African States (CEEAS) were also invited to participate in the validation workshops. English, French and Portuguese versions of the document were prepared for the workshop participants to critically review and ensure alignment of stated HIE guidelines and standards with existing Member States' national guidelines and standards. Following the validation exercise, comments and recommendations from MS were addressed and incorporated accordingly.

Introduction

The 26th Ordinary Assembly of Heads of State and Government of the AU established the Africa CDC in January 2016, and it was officially launched on 31 January 2017 in Addis Ababa, Ethiopia. The Africa CDC is working towards addressing the health challenges that the continent is currently facing as well as strengthening the capacity and capability of Africa's public health institutions to detect and respond quickly and effectively to disease threats and outbreaks using interventions and programs that are driven by evidence.

The institution is guided by the principles of leadership, credibility, ownership, delegated authority, timely dissemination of information, and transparency [1]. It acts as a forum in which Member States can discuss and trade information regarding public health interventions, as well as lessons learned from those interventions. In addition to this, it is required to function within a framework that facilitates access to obtain essential information by:

a) Establishing a continental framework for data sharing;

b) Improving data quality;

c) Developing interchangeable data elements that prepare the AU Member States to respond to emergencies; and

d) Timely disseminating critical information to the Member States.

Africa CDC developed a strategic plan (2017 – 2021) within this framework through a consultative process and situational assessment of AU policy frameworks [1]. According to the plan, one of the functional pillars of the Africa CDC will be the development and strengthening of information systems that support public health strategies in Africa. One of Africa CDC’s strategic goals is to design and operationalize a continental data-sharing platform for AU Member States. This will be accomplished by connecting the National Public Health Institutes (NPHIs) or institutions with comparable functions in each nation to a wide area network for the purpose of ensuring the safe electronic transmission of health-related data and reports. In order to accomplish this goal, it is necessary to develop an HIE guidelines and standards that will make it possible for digital health systems to be successfully implemented across the African continent.

Purpose and Scope of the Document

This document suggests guidelines and standards for the AU Member States to help develop and implement HIE for digital health systems within the African continent. While the AU Member States may use a combination of both paper-based and digital exchange solutions for interactions with the Africa CDC, this document focuses on electronic data, data exchange and security standards to assist Africa CDC in defining and specifying a framework to guide its, and AU Member States', long term development and implementation of digital health systems. The document includes:

1. A set of principles and guidelines on HIE for digital health systems;
2. A set of principles and guidelines informing HIE standards for digital health systems;
3. An HIE implementation framework for digital health systems.

Section A: Africa Union Health Information Exchange Guidelines for Digital Health Systems

To facilitate HIE for digital health systems among the AU Member States, there is a need to define the governance and legal framework for policies and standards by balancing privacy and security and data sharing needs. This section provides a set of guidelines for HIE.

Guidelines Framework

1. Governance

This sub-section provides a common set of behaviors, guidelines, and standards that enable the establishment and oversight of an effective HIE. It focuses on HIE for digital health systems on the African continent to address challenges pertaining to the exchange of health information among NPHIs or their equivalents across the continent.

1.1. Governance framework

HIE often requires complex technical and guideline choices. It needs consensus among multiple stakeholders. To establish and oversee a common set of behaviors, policies, and standards that enable HIE for digital health systems for the AU Member States, there is a need to develop an HIE governance framework. Such a framework promotes partnership and collaboration among the AU Member States to address coordination and harmonization of regulations on emerging and endemic diseases as well as public health emergencies. Therefore, the governance framework aims to serve as guiding principles of the HIE for the digital health systems of the AU Member States. The framework includes:

I. Principles for HIE governance

- AU Member States-centered
- Inclusive participation, adequate representation, and shared responsibilities
- Collaboration and/or partnership with relevant stakeholders
- National ownership of the health information that facilitates transparent bi-directional exchange with Africa CDC and the AU Member States

- Build capacity (e.g. continuous education and training) to implement the HIE agenda in the AU Member States
- Promote transparency and public accountability
- Comply with laws and regulations of AU Member States
- Promote and support innovation

II. Operational environment

- The AU HIE Guidelines and Standards shall be the preferred approach for continental HIE for digital health systems.
- The AU Member States shall support the HIE with strong incentives to vigorously promote adoption.
- The HIE for digital health systems of the AU Member States shall provide maximum flexibility for innovation and adaptation.
- AU member states shall guarantee pool of experts for the successful implementation of AU HIE Guidelines and Standards

III. Leadership

- Africa CDC shall establish fundamental conditions for trust and interoperability and shall ensure compliance.
- Africa CDC shall recognize existing HIE policies and standards across all the AU Member States and facilitate coordination and harmonization of these policies and standards with the AU HIE guidelines and standards as needed.
- The AU Member States shall participate fully and directly in the HIE for digital health systems and its governance.
- The AU Member States shall have shared responsibilities together with Africa CDC in the HIE for digital health systems

IV. Accountability

- Africa CDC and the AU Member States shall monitor and highlight innovation for the successful implementation of AU HIE Guidelines and Standards

- Africa CDC and the AU Member States shall address governance barriers
- Africa CDC and the AU Member States shall provide ongoing evaluation and continuous improvement of HIE among the Member States

V. Governance body

- Africa CDC shall establish a "Community of Practice" ("the CoP") composed of the AU Member States' representatives and other volunteer subject matter experts in Africa.
- The CoP shall oversee the AU HIE Guidelines and Standards for digital health systems and forward its recommendation to Africa CDC.
- The CoP shall elect a coordinator to oversee the day-to-day activities of the CoP.
- The CoP shall have a secretariat in the Division of Surveillance and Disease Intelligence of the Africa CDC.
- The CoP shall meet annually. The date, time, location, and agenda of such meetings shall be notified to all members at least a month in advance. In addition to the yearly meeting, the CoP may also have an emergency meeting. All meetings of the CoP shall be overseen by the coordinator of the CoP.
- The CoP shall establish a "Technical Working Group" ("the TWG") consisted of representatives from the CoP who are health, animal science or health informatics-related professionals as the governing and decision-making body for the HIE of digital health systems. Members of the TWG can also include representatives from specific domains (e.g. environmental science) as required.
- The CoP shall elect a chairperson to oversee the day-to-day activities of the TWG.
- The CoP shall elect a secretary to assist the chairperson in coordinating and performing the day-to-day activities of the TWG.
- The actions of the TWG shall be subject to review and approval by the CoP.
- The TWG shall meet every six months. Notice of the date, time, location, and agenda of such meetings shall be provided to all members at least a month in advance. In addition to the periodic meeting, the TWG may also have an emergency meeting, for example, when responding to continental public health issues. All meetings of the TWG shall be overseen by a chairperson appointed by the CoP.

- The TWG shall be responsible for providing oversight for, and strategic direction to, the AU Member States HIE for digital health systems. The TWG shall also be responsible for the HIE sustainability and scalability in both technology and services. Oversight shall include, but not be limited to, the following areas:
  a) Development, revision and approval of HIE policies and standards for digital health systems, participation agreement, standardized data sharing agreement, and HIE use cases.
  b) Development and approval of capacity building and evaluation functions.
  c) Registration of new participants (AU Member States) for the exchange of health information among AU Member States.
  d) Specification and approval of new HIE for digital health systems data types, data vocabulary terms and any related shared data registries.
  e) Ensure allocation of resources (with the support of Africa CDC), and/or the formation of sub-committees, for system and/or process improvements and evolution.
  f) Tracking and resolution of participant issues and escalation of those issues to the executive board of Africa CDC where higher-level guidance and action are needed.
  g) Selection and approval of Africa CDC digital health systems and HIE technology, equipment, platforms and interconnections.
  h) Monitor and evaluate the implementation of the AU HIE Guidelines and Standards for digital health systems in the AU Member States.
  i) Recommend Member States to develop their strategic plan considering AU HIE Guidelines and Standards.

1.2. Legal framework

In order to properly direct HIE policies for digital health systems, the development and adoption of a legal framework by each and every AU Member state is essential. This legal framework has been established with the intention of ensuring that each participating NPHI or its equivalent from AU Member States will, at all times, comply with all of the HIE guidelines policies and standards, as well as applicable state and local laws and regulations. This includes, but is not limited to, the protection of the confidentiality and security of health information.

The legal framework includes:

I. Stewardship

- The Technical Working Group (TWG) for the HIE Guidelines and Standards (specified in Section 1.1 (v)) shall review the HIE guidelines for digital health systems every two years and make such changes as appropriate, as determined by the TWG.
- Each AU Member State shall use reasonable efforts to stay abreast of any changes or updates to, and interpretations of, all applicable national, state and local laws and regulations that may affect their use and disclosure of health information.
- Each AU Member State shall allow electronic documents and messages to be equivalent to paper-based documents for legal purposes; and the source of the electronic documents and messages shall be traceable.
- Each AU Member State shall accept trusted electronic signatures as equivalent to acceptable replacements for manual signatures on paper for legal purposes.

II. Data sharing

- Africa CDC and the AU Member States should define a standard data sharing agreement for use and signature by Africa CDC and each Member State.
- In accordance with the terms of a standard data sharing agreement, each member state of the African Union (AU) is required to share electronically anonymized case-based and aggregate public health data with the Africa CDC, the other member states of the AU, and international health organizations.
- Each AU Member State shall share electronic identifiable case-based data with Africa CDC and the other AU Member States as specified in a standard data sharing agreement.

  Each member of AU Member State is obligated, when necessary, to make a request for a waiver from any specific data sharing guidelinespolicy requirement, but they are also required to provide a plan to eventually comply with that requirement over the course of time.

III. Privacy and security

- Each AU Member State shall be advised to legislate or regulate against behaviors that subvert public health systems and/or data integrity and/or data privacy.
- Each AU Member State shall define minimum-required privacy and security protections for public health data stored outside of the Member State boundaries (e.g. in a cloud environment).

IV. Domestication

- Each AU Member State shall be responsible for ensuring it is compliant with the most recent version of this HIE guidelines, which shall be made available to all AU Member State through Africa CDC.
- This HIE guidelines shall go into effect upon approval by the Community of Practice (CoP) and shall be binding once Member States sign a participation agreement with Africa CDC.

2. Continental Data Exchange Architecture, Reporting, and Sharing

The conceptual continental HIE architecture for digital health systems is a high-level architecture that defines the health data exchange beginning from the facility-level health information system and continuing all the way to the Africa CDC, WHO, regional bodies, AU Member States, and other partners. The conceptual model of the AU Member States HIE architecture is going to be discussed in the following section.

2.1. Data exchange architecture and interoperability

The AU Member States HIE for digital health architecture shall provide a common set of platforms, services and repositories for shared public health data. Data in the repositories shall be partitioned such that each AU Member State controls its own digital health data and the timing of any subsequent release of that data, or a subset of that data, to Africa CDC and/or other AU Member states' repositories. Once released, shared data can be accessed by Africa CDC and the AU Member States in accordance with signed public health data sharing agreements.

Associated services for HIE of digital health functions shall be based on interoperable software components and shall ensure that public health data from participating NPHI or equivalent are appropriately protected and controlled. A diagrammatic representation of the architecture is shown in Figure 1 below.

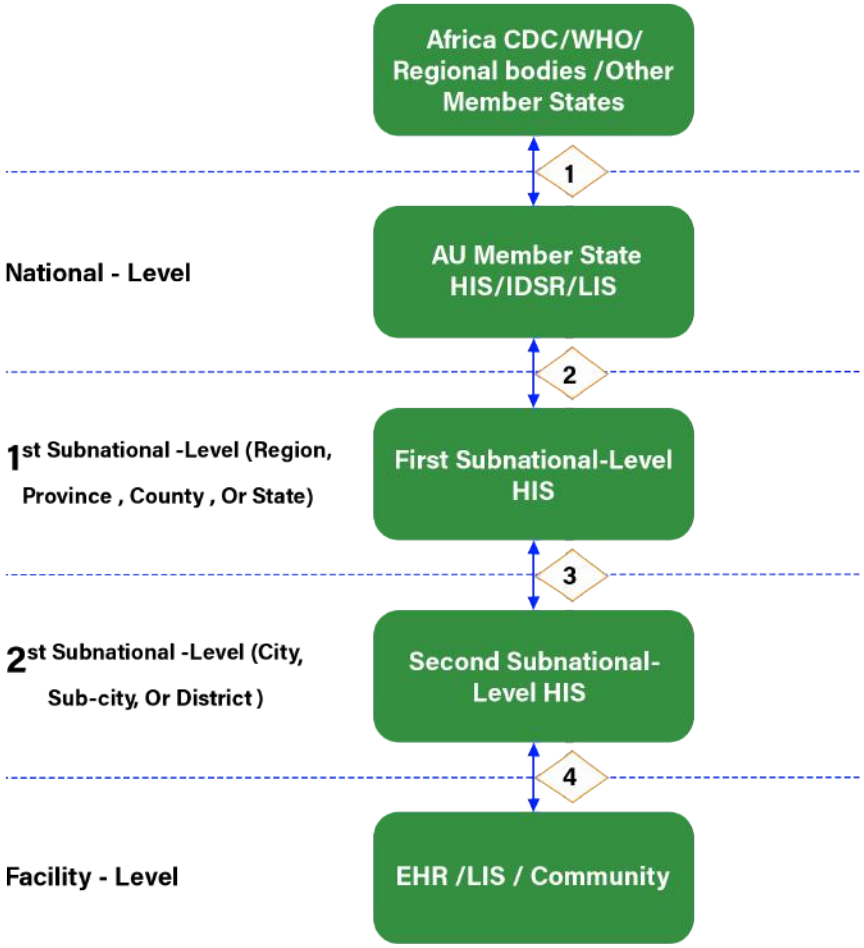
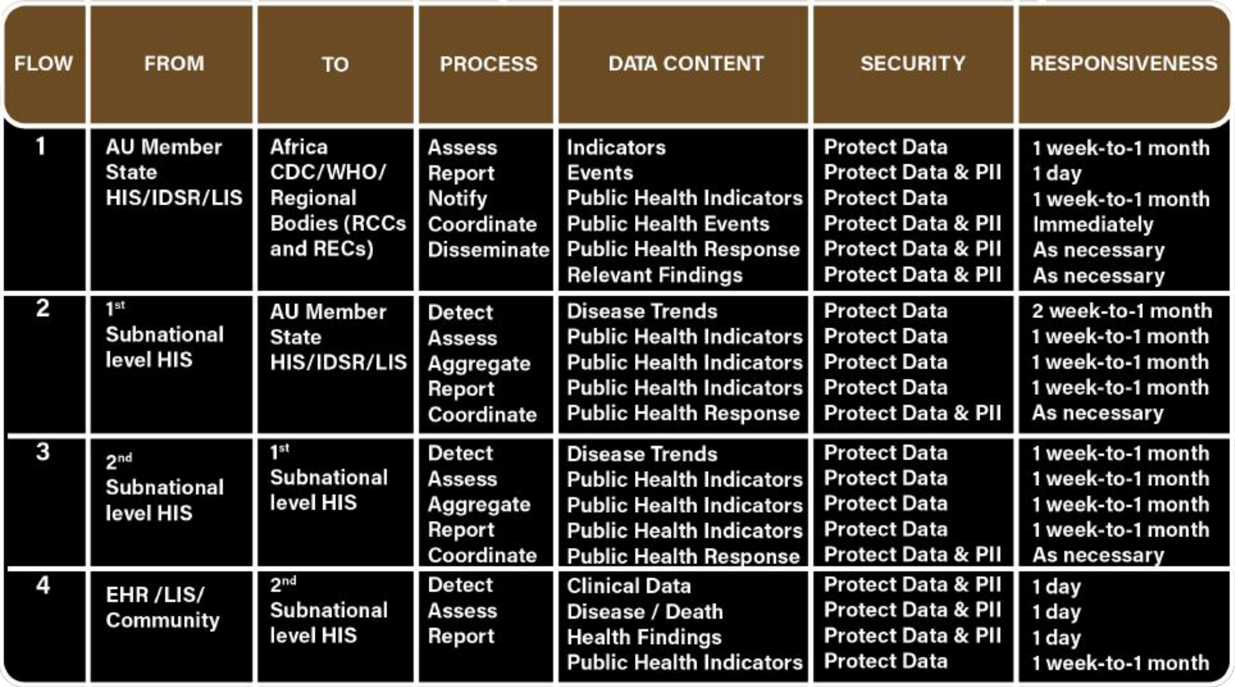

Africa CDC/WHO/ Regional bodies /Other Member States
1
National - Level
AU Member State HIS/IDSR/LIS
2
1st Subnational -Level (Region, Province , County , Or State)
First Subnational-Level HIS
3
2st Subnational -Level (City, Sub-city, Or District)
Second Subnational-Level HIS
4
Facility - Level
EHR /LIS / Community

Figure 1: AU Member States HIE Conceptual Model

Figure 1 shows the information flows starting from a facility-level health information system to Africa CDC, WHO, and African regional bodies (e.g. Regional Collaborating Committees (RCC) and Regional Economic Communities (REC)). The numbers 1 through 4 identify individual information flows. The flows numbered 1 and 2 shall be facilitated by the AU Member States digital health system encompassing the National Health Information System, Integrated Disease Surveillance and Response (IDSR), and Laboratory Information System (LIS) functionality.

The flows numbered 2 through 4 will be facilitated by the AU Member States HIE system. The details for each of these flows are described in Table 1 below.

Table 1: AU Member States HIE Conceptual Model Data Flow Definitions



FLOW	FROM	TO	PROCESS	DATA CONTENT	SECURITY	RESPONSIVENESS
1	AU Member State HIS/IDSR/LIS	Africa CDC/WHO/ Regional Bodies (RCCs and RECs)	Assess Report Notify Coordinate Disseminate	Indicators Events Public Health Indicators Public Health Events Public Health Response Relevant Findings	Protect Data Protect Data & PII Protect Data Protect Data & PII Protect Data & PII Protect Data & PII	1 week-to-1 month 1 day 1 week-to-1 month Immediately As necessary As necessary
2	1st Subnational level HIS	AU Member State HIS/IDSR/LIS	Detect Assess Aggregate Report Coordinate	Disease Trends Public Health Indicators Public Health Indicators Public Health Indicators Public Health Response	Protect Data Protect Data Protect Data Protect Data Protect Data & PII	2 week-to-1 month 1 week-to-1 month 1 week-to-1 month 1 week-to-1 month As necessary
3	2nd Subnational level HIS	1st Subnational level HIS	Detect Assess Aggregate Report Coordinate	Disease Trends Public Health Indicators Public Health Indicators Public Health Indicators Public Health Response	Protect Data Protect Data Protect Data Protect Data Protect Data & PII	1 week-to-1 month 1 week-to-1 month 1 week-to-1 month 1 week-to-1 month As necessary
4	EHR /LIS/ Community	2nd Subnational level HIS	Detect Assess Report	Clinical Data Disease / Death Health Findings Public Health Indicators	Protect Data & PII Protect Data & PII Protect Data & PII Protect Data	1 day 1 day 1 day 1 week-to-1 month

PII: Personal Identifiable Information, HIS: Health Information System, EHR: Electronic Health Record, LIS: Laboratory Information System, IDSR: Integrated Disease Surveillance and Response, RCCs: Regional Coordinating Centers, RECs: Regional Economic Communities

In table 1 the "**from**" column indicates the initiator of the data exchange flow. Once the flowis initiated, the actual data exchange will be two-way. Each flow includes one or more processes (as shown in the "**process"** column). For each process listed, there is a corresponding **Data Content**, **Security**, and **Responsiveness** requirement.

Although the detailed type of data to be reported are indicated in Table 1, priority shall be given to mortalities, clinical data, laboratory results, notifiable disease surveillance, integrated disease surveillance, and real-time national surveillance. Other reports such as logistics, genomics of viruses, and human resources can be also considered.

The AU Member States HIE for digital health platform shall exchange data based on the standards identified in Section B – AU HIE Standards for digital health Systems. The platform shall support public health data exchange among the AU Member States and Africa CDC to include:

a) Aggregated data exchange
   - From the AU Member States
   - Based on a continental Facility and Location Registry
   - *Aggregated data, from the extraction, transformation and analysis of data*

b) Entity-based data exchange (i.e., case-based patient, case, lab sample)
   - Extracted from case-based data provided to the AU Member States
   - Reducible to aggregate indicators

c) Hybrid data exchange (i.e., a mix of aggregated and entity-based data exchange)
   - Based on a combination of aggregate and case-based information
   - Initially, data may arrive in aggregated form, with aggregated and case-based transactional messages coming from more advanced AU Member State health systems.

In addition to building the continental HIE for digital health systems, the Africa CDC will provide strategic direction and promote public health practice in the AU Member States by building capacity, promoting continuous quality improvement in the delivery of public health services, and preventing public health emergencies and threats. Africa's CDC will coordinate and harmonize national health laws and programs, as well as the best ways to share health information.

The Africa CDC in collaboration and consultation with Representatives of the Member States shall define a common repository of vocabulary and terminology to be used for the HIE of digital health systems. The AU Member States will need to either adopt these vocabulary terms or map their internally used terms to these terms to facilitate shared data exchange. The continental medical vocabulary and coding terminology shall be selected and approved by the Committee based on AU Member States' inputs.

Future of the data exchange architecture

In addition to aggregate and entity-based data exchange as noted above, future evolutions of the HIE for digital health architecture shall consider genomic, veterinary, and port-of-entry public health data exchange, environmental data linkages, and anonymized population linkages as determined by the Committee in coordination with the AU Member states.

2.2. Data reporting

The data to be reported via the AU Member States HIE for digital health systems shall be linked to specific use cases defining data to be collected, data exchange content, associated vocabularies and reporting timelines. Where case-based data is reported, data sharing at the continental level will be limited in accordance with the current data sharing agreement to enable both regional and continental responses to public health situations. Data sharing may be to non-governmental organizations that fund certain treatments (e.g., antiretroviral therapy) or to the Africa CDC to enable the continent to apply for funds that could support greater investment in research at African universities (e.g., HIV research). Such data sharing arrangements can be made at AU Member States, Africa CDC or both AU member States and Africa CDC levels.

2.3. Data ownership and use agreements

I. Data ownership

In 2014, the AU adopted the African Union Convention on Cyber Security and Personal Data Protection [2] and, today, many African countries have passed data protection laws [3]. Some countries have adopted independent laws, such as the South African Protection of Personal Information Act [4] (POPIA), while other countries, such as Kenya, have adopted laws in line with the EU General Data Protection Act [5]. Arguments have been presented for strict ownership by patients of data [6] while others have presented shared ownership models [7]. Information on early concepts in data ownership [8] and the concept of clinical data ownership [7] is available in the references. For the purpose of HIE for digital health systems, the AU Member States own their own data and need to enter into data sharing and use agreements in order to share datasets. Data sharing agreements are addressed in section 2.4.

II. Data use agreement

The Data Use Agreement (DUA) can be defined as: “a contractual document used for the transfer of data that has been developed by nonprofit, government or private industry, where the data are nonpublic or are otherwise subject to some restrictions on their use”[9].

The DUA is required under privacy rules and must be entered into before there is any use or disclosure of a limited data set to an outside institution or party. A limited data set is a data set that is stripped of certain direct identifiers specified in the privacy rule. A limited data set may be disclosed to an outside party without a patient’s authorization only if the purpose of the disclosure is for research, public health, or health care operations purposes and the person or entity receiving the information signs a DUA with the covered entity or its business associate [10].

A limited data set is still protected health information (PHI), and for that reason, Africa CDC and the AU Member States must enter into a DUA with any recipient of a limited data set from each other. At a minimum, the DUA shall contain provisions that address the following:

- Establish the permitted uses and disclosures of the limited data set.
- Identify who may use or receive the information.
- Prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as otherwise permitted by law.
- Require the recipient to use appropriate safeguards to prevent unauthorized use or disclosure not contemplated by the agreement.
- Require the recipient to report to the covered entity any use or disclosure to which it becomes aware.
- Require the recipients to ensure that any agents (including any subcontractors) to whom it discloses the information will agree to the same restrictions as provided in the agreement.
- Prohibit the recipient from identifying the information or contacting the individuals.

Africa CDC in collaboration with the AU Member States shall establish a mechanism to trace data use after sharing data to users. Additionally, covered entities shall take all reasonable steps to mitigate a recipient's breach of the DUA which might involve credit repair or monitoring.

III. Data quality, integrity, use, transparency, and accountability

To make the best possible decisions at the continental level, data reported by countries must be of the highest possible quality. Data quality refers to data and information that meet specific criteria to be fit for their intended use. In public health, the most desired characteristics of data quality are completeness, timeliness, and accuracy [11, 12]. In the context of HIE, data integrity is another important dimension of data quality to ensure data is not altered between the source and point of use. When data meet all these four criteria, then it can be reliably used to make decisions. Complete data are necessary to enable the use of epidemiological techniques to calculate the incidence of disease, as well as to measure outcomes such as recovery, disability and mortality. Timely data are necessary so that decisions by policymakers at national and continental levels can occur without unnecessary delay. Accuracy is crucial to ensure decisions based on the data are made with integrity. Therefore, this guideline is to ensure that health data shared by the AU Member States are complete, accurate, and available to Africa CDC and have not been altered or corrupted in an unauthorized manner.

The following requirements shall be followed to ensure data quality, integrity, use, transparency, and accountability:

- The AU Member States shall take reasonable steps to ensure that data shared through the digital health systems are accurate, complete, and up-to-date, and have not been altered or corrupted in an unauthorized manner.
- The AU Member States shall report all cases of the reportable data in accordance with international health regulations (2005) and the African Union Health Information Exchange - Guidelines and Standards for Health Information System document (current Guidelines) to Africa CDC through the agreed HIE standards. If the National Ministry knows about a case, it should be counted and reported. All details about a case that would not jeopardize confidentiality should be included in the case report.
- The AU Member States shall report cases in a timely manner to Africa CDC. Each use case (e.g., HIV and COVID-19) should specify a reasonable time period in which the Member States can identify and report a case.

- The AU Member States shall report accurate data to Africa CDC. Ministries should establish quality control processes to ensure the data they report are accurate and will require minimal correction at a later date.
- The AU Member States shall implement technical security measures to protect against unauthorized access to the data that is being transmitted over an electronic communications network or stored within a data entry device, removable storage device, computer system, data center, or cloud services.
- The AU Member States shall work collaboratively to ensure data integrity and respond in a timely fashion to requests for review or revision. Each participating NPHI or equivalent shall have the technical capability to push updates and corrections to the AU Member States HIE for digital health systems.
- Africa CDC shall communicate to the participating institutions in case of incorrect and duplicate records. Incorrect and duplicate records shall be resolved by the participating institutions.
- Periodic audits of the AU Member States HIE for digital health data shall be conducted by Africa CDC for data accuracy, completeness, timeliness, and consistency based on standardized data quality assessment guidelines which shall be prepared by Africa CDC.
- All disclosures of data through the AU Member States HIE for digital health and the use of information obtained from it shall be consistent with all applicable national, state, and local laws and regulations, and shall not be used for any unlawful or unauthorized purpose (e.g., exposure of personally identifiable information, identity theft, and targeting for harassment).
- The AU Member States HIE for digital health systems shall operate with transparency and openness.
- Africa CDC shall be accountable for the data repository update and management.
- The AU Member States shall be accountable for ensuring data quality and timely data sharing on an agreed format.

Each AU Member State is recommended to establish a guideline for "records and information management' that specifies the following:

- Which data and information (records) will be collected by various entities (e.g., district hospital, regional hospital, and ministry) within the nation.
- In which information system records will be maintained; these can be electronic or paper-based systems.
- Ownership of the records.
- Who will have access to input and/or retrieve records from the information system.
- How access to information is traced, so that information exists to determine the cause of breach or process failure.
- How the information system will be secured to protect the privacy and confidentiality of the individuals to whom they pertain.
- The length of time records must be maintained by the organizations that manage them.
- Under what conditions a record may be expunged, deleted, or archived.
- What are the acceptable methods for data disposal.
- For what purposes the records may be used.

2.4. Open data

The Open Data Handbook provides "data that can be freely used, re-used and redistributed by anyone - subject only, at most, to the requirement to attribute and share alike" [13]. The full open data definition [13] provides additional criteria, including Availability and Access, Re-use and Redistribution, Universal Participation and Interoperability. Open data models can play an important role in creating a framework for providing interoperable data services that support the development of innovative Smart Health applications profiting from data fusion and sharing [14]. For HIE purposes, non-identifiable data shared among the AU Member States and Africa CDC shall be treated as Open Data within this continental community. Data use beyond this community must be specified in a data use agreement (see Section 2.3).

Inspired by Open Science, there are FAIR guiding principles, which are now being advocated by information science communities [15]. FAIR intended to provide guidelines to improve the Findability, Accessibility, Interoperability, and Reuse of digital assets. FAIR is not equal to Open [16]. The 'A' in FAIR stands for 'Accessible under well-defined conditions'. Sometimes, there may be legitimate and valid reasons to shield data and services generated with public funding from public access. These include personal privacy, national security, and competitiveness.

I. Open data guideline

The Africa CDC shall establish a Data Management and Sharing Policy [17]. The Open Sunlight Foundation's Open Data Policy Guidelines [18] shall be adopted by the Africa CDC for this use.

II. Purpose of the open data guideline

The open data guideline shall ensure that participating Member States identify, prepare and publish relevant, accurate, high-quality datasets within and across AU Member States and with Africa CDC in a timely manner [19]. The Open Data guideline shall provide the opportunity for the Member States to update and improve access to information that is already open, and to specify new datasets and records be collected and published.

III. Types of data that can be shared to users

Public health data are a key element for sharing. A guide published by the Centre on Global Health Security in 2017 [20] states that sharing public health data improves and protects public health. It can help to achieve the UN SDGs, particularly SDG 3 – “to ensure healthy lives and promote well-being for all at all ages.” Africa CDC in agreement with the AU Member States shall specify the public health data to be shared among the AU Member States and Africa CDC in a data sharing agreement. An AU Member State shall have the ability to request a temporary waiver from sharing a particular set of data whenever necessary but shall also provide a plan and timeframe for being able to share the particular data.

IV. Principles of data sharing

The World Data System Scientific Committee published data sharing principles in line with the data policies of a number of national and international initiatives [21]. The Data Sharing Principles in Developing Countries (The Nairobi Data Sharing Principles) have also been published [22].

The Africa CDC data sharing guideline shall specify data-sharing principles as an important way to increase the ability of researchers, scientists and policy-makers to analyze and translate data into meaningful reports and knowledge.

Accountability

Sharing data requires trust and accountability between partners. Trust is built over time and accountability is developed through strong data-sharing agreements and ensuring that data are used for the intended purposes. The data sharing guideline shall enable trust and require accountability among participants.

Confidentiality

Maintaining the privacy and confidentiality of individuals' information requires that any shared data be either anonymized or protected from unauthorized use, access, and disclosure to the greatest extent possible. Confidentiality ensures that this protection takes place. The data sharing guideline shall specify that all shared entity-based data shall be strongly protected to prevent the disclosure of personally identifiable information. The policy governing the sharing of data must stipulate that all entity-based data that is shared be subject to stringent protection. The method of data collection, in addition to all of the necessary procedures for data sharing, and meta data, are all responsibilities of AU Member States. .

Data Quality

Open data can improve the quality of data by opening it up to scrutiny by others. The data sharing guideline shall specify when AU Member States’ shared data may be used freely by Africa CDC and other Member States.

Efficiency

Shared data results in increased efficiencies in terms of reducing duplication of effort in capturing and acquiring data. The data sharing guideline shall specify where shared data will be made available to users.

V. The data sharing agreement

Examples exist for provisions included in a typical data-sharing agreement [23] and for guides to sharing public health data [20]. A recent paper from South Africa articulates the use of a Material Transfer Agreement to share data [24].

The Africa CDC data sharing agreement shall be a formal contract that clearly documents what data are being shared and how the data can be used. The agreement shall serve two purposes. First, it shall protect the data provider, ensuring that the data will not be misused. Second, it shall prevent miscommunication on the part of the provider of the data and the data recipient by establishing the parameters of data use. Each AU Member shall complete a data sharing agreement with Africa CDC. Each agreement shall be subject to zero or more temporary waivers for provisions that the AU Member State is not able to meet at the time of signing. All waivers shall include a plan and timeframe for resolution. Africa CDC shall ensure that all such waivers are resolved in accordance with the AU Member States provided plan and timeframe.

There shall be four main components to the data sharing agreement: defining the data to be shared, securing the shared data, complying with any and all legal requirements on the data, and specifying the conditions under which data may be shared with external entities other than the data sharing participants.

The following items shall be included in the data sharing agreement:

- Period of agreement
- Intended use of the data
- Constraints on the use of the data
- Data confidentiality
- Data security
- Methods of data-sharing
- Financial costs of data-sharing
- Any other items to be decided by Africa CDC and Member State

A data sharing and use agreement template is annexed in the Annexure 14.

2.5. Data privacy and security policies

Healthcare organizations are vulnerable to internal and external security threats due to the value of health information; thus, protecting health information is challenging [25]. It is important to note that privacy, security and confidentiality establish the trust necessary for successful digital health system interoperability [26].

Approximately 57% of the AU Member States (31) either have privacy and data protection legislation in place or are presently drafting their e-privacy and data protection legislation [27]. However, regarding health data privacy and security standards, the following challenges have been observed: lack of legal frameworks in place to support privacy and security of health data; lack of national-level governance bodies; wrong cultural attitude toward patient confidentiality; the existence of non-health-specific privacy laws that cannot be interpolated for health data [28]. Significant privacy and security actions include granting data access to users at a national and continental level, establishing the privacy and security protocols, understanding the current security conditions and solutions, and selecting the appropriate patient identification and authentication standards.

Africa CDC values the importance of establishing and maintaining solid data privacy and security policies within its organization and partner organizations including the AU Member States. Data privacy and security policies enable organizations to establish standards, rules, and regulations around securing data and maintaining confidentiality and safeguarding against potential breaches.

Whether health information resides in paper or electronic form, personally identifiable information (PII) must be secured to protect both data and patient's privacy. In the case of electronic public health data, while most day-to-day public health data will be anonymized, access to PII will be required to support public health case tracking activities for those diseases with high epidemic potential to cause serious public health impact due to their ability to spread rapidly both nationally and internationally (e.g., cholera, plague, yellow fever, viral hemorrhagic fever, and COVID-19).

I. AU conventions

The African Union adopted a Convention on Cybersecurity and Personal Data Protection in June 2014. The Convention states that the mechanism so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State and the rights of local communities. Furthermore, data collection shall be undertaken for specific, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes; data collection shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed; data shall be kept for no longer than is necessary for the purposes for which the data were collected or further processed; personal data shall be processed confidentially and protected, in particular where the processing involves the transmission of the data over a network; the processing of personal data shall be confidential. Such processing shall be undertaken solely by persons operating under the authority of a data controller and only on instructions from the controller.

II. National laws, regulations, and other policies

As specified in the AU Convention on Cybersecurity and Personal Data Protection[1], data privacy and security policies, including those of Africa CDC, shall comply with national laws, regulations, and other policies of AU Member States. Each State Party shall commit itself to establish a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of the free flow of personal data. State Parties shall also adopt the strategies they deem appropriate and adequate to implement the national cybersecurity guideline, particularly in the area of legislative reform and development, sensitization and capacity-building, public-private partnership, and international cooperation, among other things. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cybersecurity guideline and lay the foundation for effective management of cybersecurity incidents and international cooperation. Legislation on privacy and data protection already exists for many of the AU Member States.

III. Mechanisms ensuring data confidentiality, integrity, and availability

The following mechanisms shall be adopted by Africa CDC to ensure data privacy, confidentiality, integrity and availability:

- Always protect AU Member States' public health data.

[1] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

- Collect and process what is needed and important, and nothing else - each data element must be justified.
- Maintain and preserve information and associated information management and exchange infrastructure to prevent corruption and/or unauthorized change (e.g., password-protected information systems, access restriction to authorized users, secured and locked storage of paper data collection forms and health facility registries, etc.)
- All systems (i.e., servers, personal computers/laptops and mobile devices) accessing the Africa CDC should include firewall, virus protection, and data loss prevention solutions. These systems should further install the latest available updates for their respective operating system, virus definitions, and software security.
- Ensure that all Africa CDC and AU Member States national system data are anonymized to the maximum extent possible to include both indicator-based, event-based, and case-based data.
- Establish a common definition for PII across all the AU Member States.
- Limit exposure of PII to situations where such exposure is deemed critical and necessary to the performance of public health safety actions (e.g., cross-border security issues and/or cross-border public health emergencies (i.e., in the public interest)).
- Protect patient PII - infant, child, adolescent, adult, senior citizen, male/female, key populations.
- Strongly encrypt all public health message content both at rest and in transit.
- All systems handling HIE data should provide tools for data encryption (both at rest and in transit) and data backup.
- Obtain pre-approval from AU Member State data control authority prior to exchange of de-identified data (i.e., must have an approved source), based on pre-established confidentiality agreements between Africa CDC and the individual AU Member States.
- Always encrypt PII when present.
- Always use anonymous, unique identifiers whenever possible (i.e., de-identified data); separately secure and encrypt any mapping between anonymous unique identifiers and actual patient identities and restrict access to such mapping to only trusted and vetted

personnel.

- Establish mechanisms to detect and notify appropriate authorities of data breaches and infrastructure compromises.
- Establish Africa CDC and AU Member State Computer Emergency Response Teams (CERTs) or the Computer Security Incident Response Teams (CSIRTs) to respond to cyber threats, data breaches, and system outages.

IV. Data breach reporting and remediation

Data breaches refer to the unauthorized disclosure and acquisition of personal data from an information system. As specified in the AU Convention on Cybersecurity and Personal Data Protection[2] regarding data breach reporting and remediation, State Parties need to invest in developing appropriate legislation to prosecute and convict cybercrimes that intercept or attempt to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system; knowingly use data obtained fraudulently from a computer system; and fraudulently procure, for oneself or another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system. In the event of a data breach, local laws and regulations of the affected AU Member States may also be applied.

Each AU Member State and Africa CDC shall strive to detect any circumstances that could lead to or result in a potential or actual breach. Africa CDC shall be required to report any breach of protected health information to the relevant AU Member States. Any AU Member State that has reason to believe that a breach has or may have occurred shall promptly report such information to Africa CDC. “Discovery” of a potential breach occurs when either Africa CDC is told by the AU Member States or other entities about a potential breach or when Africa CDC discovers a potential breach.

In the event of a public health data breach, either AU Member States or Africa CDC (depending on where the breach occurs) shall notify each other within 24 hours.

[2] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

The AU Member States must report the nature of the breach, describe the potential risk to the individuals whose data was accessed and disclosed, and specify the corrective actions taken to avoid future breaches. To review data breach reports and provide relevant guidance to the affected Member State, Africa CDC shall establish a breach investigation committee comprised of Africa CDC staff members from the Division of Surveillance and Disease Intelligence and the Science and Program Office, and other disease surveillance and health information system experts from selected Member States. Depending on the nature and severity of the reported data breach, the breach investigation committee may recommend that a risk/harm assessment be conducted in the affected Member State by members of the committee or other. The assessment should include an examination of current data privacy and security safeguards, policies, and practices to identify ongoing risks and proposed remediation to prevent future breaches from occurring. Such assessments should be conducted within 30-60 days from when the breach was reported to Africa CDC. Africa CDC shall retain all documentation regarding breaches, including copies of breach notifications sent in accordance with this guideline.

Section B: African Union HIE Standards for Digital Health Systems

This section describes current standards and technologies on HIE, data exchange standards, privacy and security standards, and common foundation standards for interoperability.

3. Review of Current Standards and Technologies related to HIE in Africa

Africa has seen a steady increase in the deployment of digital health solutions. Most of these systems use technologies that are local, proprietary, and insular [29]. Lack of interoperability, the ability to exchange data, between heterogeneous systems has been recognized as a key obstacle to realizing the potential benefits of e-health [30]. The World Health Assembly's resolutions on e-health (WHA:58.28 (2005)) [31], on ehealth standardization and interoperability (WHA:66.25 (2013)) [32], and on ehealth (WHA:71.20 (2018) [33] and WHA:71.57 (2018) [34]) all recognize the role of interoperable digital systems in achieving the SDGs.

All digital health strategies, policies and architectures reviewed among African countries mentioned standards as a key piece for interoperability and improved HIS integration [Ghana e-health strategy (2010) [35], Tanzanian National e-health Strategy (2019) [36], National Health Normative Standards Framework for Interoperability in e-health in South Africa (2014) [30], Kenya e-health Policy (2016) [37], Rwanda National e-Health Policy (2017) [38] and Ethiopian e-health Architecture (2018) [39]]. Challenges include HIE governance frameworks, regulatory e-health standards across all levels of HIEs, and national and continental coordination.

For any two or more heterogeneous systems to exchange data meaningfully, there must be a mutual standard for data exchange or communication between those systems [40]. Data exchange standards provide clear guidelines for robust and interoperable solutions [30, 41, 42]. Cognizant this, the Africa CDC HIE Task Force adopts and recommends HIE interoperability standards that can be used by the AU Member States to support various digital health systems, disease surveillance and the AU's pandemic response (such as COVID-19) among AU Member States, Africa CDC, and RCCs.

4. Data Exchange Standards

The Data Exchange Standards for digital health systems recommendations provided herein apply directly to specific boundaries as shown in Figure 1 of the Guidelines Section.

4.1. Systems standard guidelines

There is no one-size-fits-all digital solution for Africa. Instead, each solution has to be tailored to national and continental needs, circumstances and resources. Each solution should support incremental extension into a fully integrated national health information system without substantial reengineering of legacy systems [43]. It is not practical to either discard the existing systems or have only one system in place to solve the interoperability problem [29]. At the same time, Africa CDC encourages the use and application of modern technologies in order to maximize long-term benefits for AU Member States digital health systems.

The African Union countries should aspire towards a more integrated, open and flexible digital solution [44]. Specifically, common global goods have been recognized across public and private entities as a fundamental course of action towards building interoperable, cost-effective, easy-to-use infrastructure components [45].

Instead of naming specific systems, the Africa CDC recommends that the applications/platforms for health, disease surveillance, laboratory and the HIE systems chosen by the Africa CDC, AU Member states, public and private facilities to all follow the principles and practices shown in Annexure 3.

4.2. Communication protocols

The AU Member States are recommended to adopt the following communication protocols for their in-Country digital health systems communications:

- Sensor communications: Institute of Electrical and Electronics Engineers (IEEE) 11073-10101 (Nomenclature), IEEE 11073-10201™ (Domain information model) and IEEE 11073-20101™ (Application profile base standard) for supporting interoperable communication among sensor devices and computers.

- Transport layer: Internet Engineering Task Force (IETF) Internet Protocol (IP) Version 4 [RFC 1812 (IPv4 Routers) and 2474 (IPv4)] and Transmission Control Protocol (TCP) [RFC 793, 1122, 3168, 6093, 6528 and 7414] for internetworking between participants and local area networks. Use of User Datagram Protocol (UDP) [RFC 768] is not allowed for Africa CDC HIE communications.
- Transport layer security: IETF Transport Layer Security (TLS) Protocol Version 1.3 [RFC 8446] for securing FTP, Simple Mail Transfer Protocol (SMTP) and Hypertext markup language (HTTP) services.

4.3. Messaging standards

The internationally known comprehensive and robust data exchange standards are recommended.

- For public health and clinical content messaging, the following Health Level Seven (HL7) messaging standards are recommended:
  - For public health messaging: HL7 V2.5.1 is recommended as it is the most widely used clinical messaging and administrative standard to facilitate exchange of healthcare data about admission data, discharge/transfer data, orders and results of laboratory tests, treatments, clinical observations, appointment schedules, and billing information among heterogeneous healthcare systems. The main benefits of HL7 V2 are its backward compatibility and its high level of flexibility to adapt to any healthcare environment. Specifying a single HL7 messaging standard (V2.5.1) will eliminate the need to perform conversions between differing HL7 formats.
  - For clinical content and structure (including clinical summaries, discharge notes, laboratory, radiology investigation), use HL7 V3R2 Clinical Document Architecture (CDA). Additionally, Africa CDC recommends the HLT Continuity of Care Document (CCD) for the exchange of clinical information, including patient demographics, problems, medications and allergies.
  - For exchanging data for digital health and cloud communications, use IHE or HL7® Fast Healthcare Interoperability Resources (FHIR) standard cloud communications. FHIR combines the best features of HL7v2, HL7 V3R2 CDA and web standards (Extensible

    Markup Language (XML), JavaScript Object Notation (JSON), HTTP, Atom and others). Because of this, the TF recommends all new implementations and digital health system improvements use FHIR as the primary mechanism for data exchange.

    - The latest HL7 messaging standards can also be adapted.

- DICOM is used to share digital medical diagnostic images between imaging equipment and other healthcare applications. It is used for things like radiology, radiotherapy, ophthalmology, ultrasound, digital mammography, pathology, dentistry, dermatology, computed tomography, etc. It lays out the structure of the data and the rules for how medical images can be shared.
- Aggregate Data e-Xchange (ADX) profile is recommended by Africa CDC to support the exchange of health indicators, aggregate data (from District Health Information System Version 2 (DHIS2)) and metadata among AU member states [30, 46, 47].
  [See https://wiki.ihe.net/index.php/Aggregate_Data_Exchange].
- Data and document markup language: Use World Wide Web Consortium (W3C) e-Xtensible Markup Language (XML) [see https://www.w3.org/TR/xml/] for ease of processing exchanged data and document content and to identify data/document sources.
- Web page markup language: Use Use Web Hypertext Application Technology Working Group (WHATWG) and W3C Hypertext markup language (HTML) version 5 [see https://html.spec.whatwg.org] for web page presentation and development.
- Data interchange format: Use JavaScript Object Notation (JSON) [RFC 7159] [see https://tools.ietf.org/html/rfc7159] for ease of processing exchanged data and document content and to identify data/document sources.
- Transmission character sets: Use Use International Organization for Standardization (ISO) Unicode Transformation Format (UTF-8) encoding [per ISO/IEC 10646-1:2017]. This standard also conforms to ASCII encoding as used by HL7 v2.5.1.

The above messaging standards map to different Africa CDC reporting categories, as shown in Annexure 4.

4.4. Vocabulary standards

It is advised that the following standards serve as the foundation for the specification of terminology and nomenclature for HIE (these standards cover a wide range of topics, but only a portion of each will be applicable for use by the Africa CDC in digital health systems, even though broader use by the AU Member States is advised):

- Systematized Nomenclature of Medicine - Clinical Terminology (SNOMED-CT) [43, 48] for coding terms and synonyms for clinical findings, symptoms, diagnoses, procedures, pharmaceuticals, etc. It has inbuilt mechanism to cater for local extensions and different languages.
- International Classification of Disease (ICD-11) for classifying diseases, health conditions, causes of death, clinical terminology and coding standards.
- Logical Observation Identifiers Names and Codes (LOINC) for coding laboratory test reports. LOINC codes can be integrated into the data message content such as HL7 V2.5.1 and HL7 CDA for standardizing laboratory reports such as chemistry, hematology, serology, microbiology, and toxicology as well as cell counts, antibiotic susceptibilities, and others.
- RX-Norm provides normalized names for clinical drugs and links its name to many drug vocabularies commonly used in pharmacy management and drug interactions.
- Diagnostic and Statistical Manual of Mental Disorders (DSM) should be used as the nomenclature that clinicians can reference to enhance clinical practices and as a language for communicating diagnostic information.

The above vocabulary standards map to different Africa CDC reporting categories, as shown in Annexure 5.

4.5. Integration profile

For the purpose of mapping local identifiers to social security numbers, biometric identification numbers, or national identification numbers, the Africa CDC advises the establishment and management of a patient registry that contains information conforming to the HL7 V3 ADT (Admit-Discharge-Transfer) standard. Patients are only allowed to share their medical records with with service providers and the Africa CDC if they provide an informed consent [49] and or agree to take part in a study. This recommendation is made by the Africa CDC to protect patients' privacy and security and is based on the Advanced Patient Privacy Consents (APPC) profile. The data pieces that are exchanged locally are distinct from those that are exchanged across international borders. For local exchange, the major data elements that are recommended to be collected include patient demographic information, information about the facility, and patient history information including vital signs, allergies, immunization status, diagnosis case, diagnosis result, treatment, and appointment date and time. When it comes to the exchange of data across international borders, the data elements consist of aggregated data elements that place an emphasis on the critical diagnosis of cases in accordance with the guideline of the International Patient Summary (IPS) [see application beyond a specific region or country]. For the secondary use of data, the Africa CDC suggests combining national standards (if there are any) with newly established international standards (as noted in Section 4.3). This recommendation applies to secondary uses of data for both domestic and international purposes.

Disclosure of patient information for the purposes of research necessitates that the data be maintained with regard to its statistical features throughout the disclosure process in order to limit the amount of information that is lost [50]. Therefore, the Africa CDC recommends that public health researchers share flat data files (including the date of service, facilities of service, patient month and year of birth, sex, test results, vital signs, and diagnosis codes associated with the encounter) with the organization. This recommendation is contingent on a data sharing and use agreement described in , which is outlined in the policy section of the data sharing and use guideline of the guidelines section.policy. In addition, researchers are required to sign agreements that protect the confidentiality of their data.

The Africa CDC recommends the use of the following standard practices for integration of patient profiles:

- Use of unique case identifier format in order to prevent identifier collisions across the AU Member States, all case identifiers shared with the RCCs and Africa CDC should include a unique country prefix.
- Establishment of shared registry databases to include:

  - Public Health System (PHS) participants and unique identification codes; only identified AU Member States and their designated participants should have access to the AU Member States digital health registry. Unique participant codes support the anonymization of exchanged messages or data's source and/or destination.
  - PHS policies to specify allowable transactions and information access by each participant (see Section A).
  - Public health vocabulary data to support AU Member States messaging system development, sharing with potential digital health system users and dissemination of latest vocabulary and terminology information.
  - Public health information to be shared among digital health participants, or a subset of designated PHS participants (e.g., evolving disease outbreaks in neighboring AU Member State(s)).
- Report per WHO-Africa CDC agreement: Report diseases based on the latest decision instrument between the Africa CDC and the WHO:
  - Diseases reported internationally under the current International Health Regulations (IHR) [51] (e.g., smallpox, poliomyelitis due to wild-type poliovirus, human influenza caused by a new subtype, Severe Acute Respiratory Syndrome (SARS)).
  - Diseases with high epidemic potential to cause serious public health impact due to their ability to spread rapidly internationally (e.g., cholera, plague, yellow fever, viral hemorrhagic fever).
  - Diseases that are principal causes of morbidity and mortality due to communicable diseases and conditions in the African Region (e.g., malaria, pneumonia, diarrheal diseases, tuberculosis, HIV/AIDS, maternal deaths and injuries).
  - Any priority non-communicable diseases or conditions in the region (e.g., high blood pressure, diabetes mellitus, mental health and malnutrition).
- **Consolidate information from relevant sectors:** Information from relevant sectors of the administration of the Africa Union Region concerned is consolidated by RCCs. These relevant sectors include those responsible for surveillance and reporting, points of entry, public health services, laboratories, clinics, and hospitals, as well as other government departments from the AU and its Member States (per IHR Article 4.2).

- **Disseminate information to relevant parties:** Information is disseminated by RCCs to relevant sectors of the administration of the Africa Union Region concerned, such as those responsible for surveillance and reporting, points of entry, public health services, laboratories, clinics, and hospitals, as well as other government departments of the Africa Union and Africa Union Member States (per IHR Article 4.2).
- **Report expediently:** Report within twenty-four hours of completing an analysis of public health information [timeliness requirement] using the method of communication that is the most effective among those that are available (as specified in Article 6.1 of the IHR). [It is important to note that evaluation takes place at the RCC level]
- **Report public health emergency events of international concern:** Report all events which may constitute a public health emergency of international concern within its territory in accordance with the decision instrument (per IHR Article 6.1).
- **Report public health response to events:** Report any health measure implemented in response to those events (per IHR Article 6.1).
- **Protect information:** Respect the dignity, human rights and fundamental freedoms of persons (per IHR Article 3.1).

5. Privacy and Security Standards

5.1. External assessment and audits

- Africa CDC suggests that an audit log or series of audit logs be made and kept for the HIE to track:
- Participant access attempts, successes and failures: this will support the identification of unauthorized access attempts for the security audit process.
- Message sources and volumes: this will support the identification of changes in the statistical message traffic volume over time for both the security audit process and system expansion planning.
- Transaction types and volumes: this will support the identification of changes in the statistical transaction levels over time for both the security audit process, system expansion planning and system improvement prioritization.
- Participant time of access patterns: this will support the identification of unexpected HIE usage based on time of day and/or day of the week for the security audit process.

5.2. Risk management: assessment and acceptance

Africa CDC recommends:

a) Use of predictive Bayesian network analysis.
b) Elicitation of users' privacy valuation using the experimental economics operationally critical threat, asset, and vulnerability evaluation (OCTAVE) approach.
c) Putting in place an information security insurance contract [50].
d) Measuring risk level in terms of a combination of the likelihood of occurrence (probability) and degree of impact (positive or negative) (NIST SP 800-30).

5.3. Security standard

Africa CDC recommends the following technical standards for information security:

- Certificates: ITU-T X.509 digital certificates for use in public key encryption for TLS and S/MIME. To be used in conjunction with Public Key Cryptography Standards 7 (PKCS7) Cryptographic Message Syntax [IETF RFC 5652] and Public Key Cryptography Standards 12 (PKCS12) Personal Information Exchange Syntax Standard [IETF RFC 7292].
- Hashing algorithms: NIST Secure Hashing Algorithm 2 (SHA-2) to include SHA-256, SHA-384 and SHA-512 for creating a one-way secure hash of a document or message; in conjunction with PKCS7 to support the traceability of content to a trusted source [see https://csrc.nist.gov/publications/detail/fips/180/4/final].
- User assertion: XUA profile with user role, authorization and purpose of use-cases. XUA Profile is focused on Web-Services transactions that follow ITI TF-2 with a SAML 2.0 Token containing the identity Assertion [see https://wiki.ihe.net/index.php/Cross-Enterprise_User_Assertion].
- ISO security and access controls for privilege management and access control (ISO/TS 22600).
- ASTM Standard Guide for User Authentication and Authorization (ASTM E1985-98) [50].

In order to successfully secure the exchange of health information across all levels of the health system, it is imperative that the human factor, which includes things like training and awareness as well as disaster preparedness and recovery plans, be taken into consideration.

6. Common Foundation Standards for Interoperability

6.1. Standards management

Africa CDC ecommendss that each Member State should form a working group at the national level in order to continually review its standards once every two years and to ensure that these standards evolve in a manner that is both thoughtful and under control.

Messaging exchange standards test support

In order to verify messaging implementations and associated vocabularies, Africa CDC recommends the creation of a message testing environment and the development of a message validation tool to be used by all participating AU Member States.

Protocols and services for interoperability

The following interoperability service areas are critical to achieving digital health systems interoperability between the Africa CDC and the AU Member states. Each service area as briefly described below should comply with the latest version of the corresponding RFC standard or equivalent service, when and as adopted by the Africa CDC. The initially recommended standard for 2022 is identified below as the baseline for interoperability evolution over time:

Africa CDC recommends that participating systems from the AU Member States support at least one, and preferably all, of the following transfer protocols:

- File Transfer Protocol over Transport Layer Security (FTP-TLS) to support secure access to, and transfer of messages and information files. This provides one possible service alternative for data exchange (i.e., encapsulation of digital health system messages and/or documents into a machine-readable file). For 2022, the current applicable IETF protocols for FTP-TLS are RFC 959 (FTP), 2246 (TLS), 2228 (FTP Security Extensions) and 4217 (FTP-TLS).

- Simple Mail Transfer Protocol (SMTP) over Transport Layer Security (SMTP-TLS) to support secure access to, and transfer of messages and information files. This provides another possible service alternative for data exchange (i.e., encapsulation of digital health system messages and/or documents as a secure file attachment to an email). For 2022, the current applicable IETF protocols for SMTP-TLS are RFC 2246 (TLS), 3207 (SMTP-TLS), 7817 (Updated SMTP-TLS) and 8314 (TLS for Email). An email should, in turn, be supported by:
    - Secure/Multipurpose Internet Mail Extensions (S/MIME) for secure attachments to SMTP email and protection of data content (i.e., while SMTP-TLS provides encryption of data while in transit, S/MIME provides additional protection for data at rest (e.g., stored on a system). Africa CDC requires Authenticated Encryption with Associated Data (AEAD) algorithms only (i.e., with strong encryption performance). Participating systems from the AU Member States must also support this standard if supporting SMTP-TLS. For 2022, the current applicable IETF protocols for S/MIME version 4 are RFC 5652 (Cryptographic Message Syntax (CMS), 3370 (CMS Algorithms), 5754 (Secure Hashing Algorithm 2 (SHA-2)), 8702 (SHA-3) and 8551 (S/MIME).

    - Simple Object Access Protocol (SOAP) to support the exchange of information over SMTP-TLS. The AU Member States digital health systems shall support this standard (i.e., to facilitate system-to-system services exchange using SMTP-TLS). For 2022, the current applicable W3C protocol is SOAP version 1.2 messaging framework (https://www.w3.org/TR/soap12-part1/). Representational state transfer (REST) is the optional standard to support exchange of health information.
    - Hypertext markup language (HTML) for web page presentation and development. The AU Member States digital health systems shall support this standard (i.e., to facilitate the development of web pages accessible to systems over SMTP-TLS). For 2022, the current applicable WHATWG and W3C protocol is HTML version 5 [see https://html.spec.whatwg.org].

- Hypertext Transfer Protocol over Transport Layer Security (HTTP-TLS) to support a secure web access to, and transfer of, messages and information files. This provides a third possible service alternative for data exchange (i.e., between two systems or between a user and a web application). For 2022, the currently applicable IETF protocols for HTTP-TLS are RFC 2817 (TLS within HTTP), 2818 (HTTP-TLS), 7230 (HTTP Syntax & Routing), 7595 (Universal Resource Locators (URIs)) and 8615 (Well Known URIs). HTTP-TLS should also be supported via:
    - Representational State Transfer (REST) to support access (GET, POST, PUT, PATCH and DELETE) to predefined web site links and associated resources and/or data (i.e., to facilitate system-to-system and user-to-system services exchange using HTTP-TLS). At a minimum, the AU Member States digital health systems shall support this architectural approach for access to registry databases. For 2022, the current applicable IETF protocol for REST is RFC 6690 [see also https://tools.ietf.org/id/draft-keranen-t2trg-rest-iot-05.html].
    - Simple Object Access Protocol (SOAP) to support the exchange of information over HTTP-TLS or SMTP-TLS. The AU Member States digital health systems shall support this standard (i.e., to facilitate system-to-system services exchange using HTTP-TLS). For 2022, the current applicable W3C protocol is SOAP version 1.2 messaging framework (https://www.w3.org/TR/soap12-part1/).
    - Hypertext markup language (HTML) for web page presentation and development. The AU Member States digital health systems shall support this standard (i.e., to facilitate development of web pages accessible to users as well as to systems over HTTP-TLS). For 2022, the current applicable WHATWG and W3C protocol is HTML version 5 [see https://html.spec.whatwg.org].

Section C: African Union HIE Implementation Framework: A Case of Electronic Disease Surveillance

This section highlights the implementation by way of illustration. It also discusses how the HIE guidelines and standards have been put into practice through the use of electronic disease surveillance. Cloud computing and shared services; the creation of new infrastructure; the enhancement of existing capacities; monitoring, evaluation, and research; In addition, this section emphasizes the positive effects that the HIE of AU Member States can have on digital health systems.

HIE for e-Surveillance Benefits

The initial implementation of the AU Member States HIE for e-Surveillance shall provide benefits in the following:

a) Response time

- Rapid and timely transmission of data from lower data sources (facilities and labs) to higher levels (sub-national and national), enabling appropriate public health action(s).
- Faster automated data processing, analysis and reporting.
- Improved speed of outbreak detection due to earlier alert.
- Improved the ability to determine the time, persons and place factors of an outbreak enabling more effective prevention and control measures.

b) Data exchange

- Common data structure and format improving data accessibility, use and interpretation.
- More consistent data collection through standardized automated tools.
- Ease of data exchange and comparison across health facilities through data standardization.
- Ability to leverage common and rich datasets across multiple public health entities via data interoperability and sharing.

c) Data quality

- Shared standards and workflow provide interoperability with other information systems.
- Improved data quality through automated validation.

d) Monitoring and evaluation

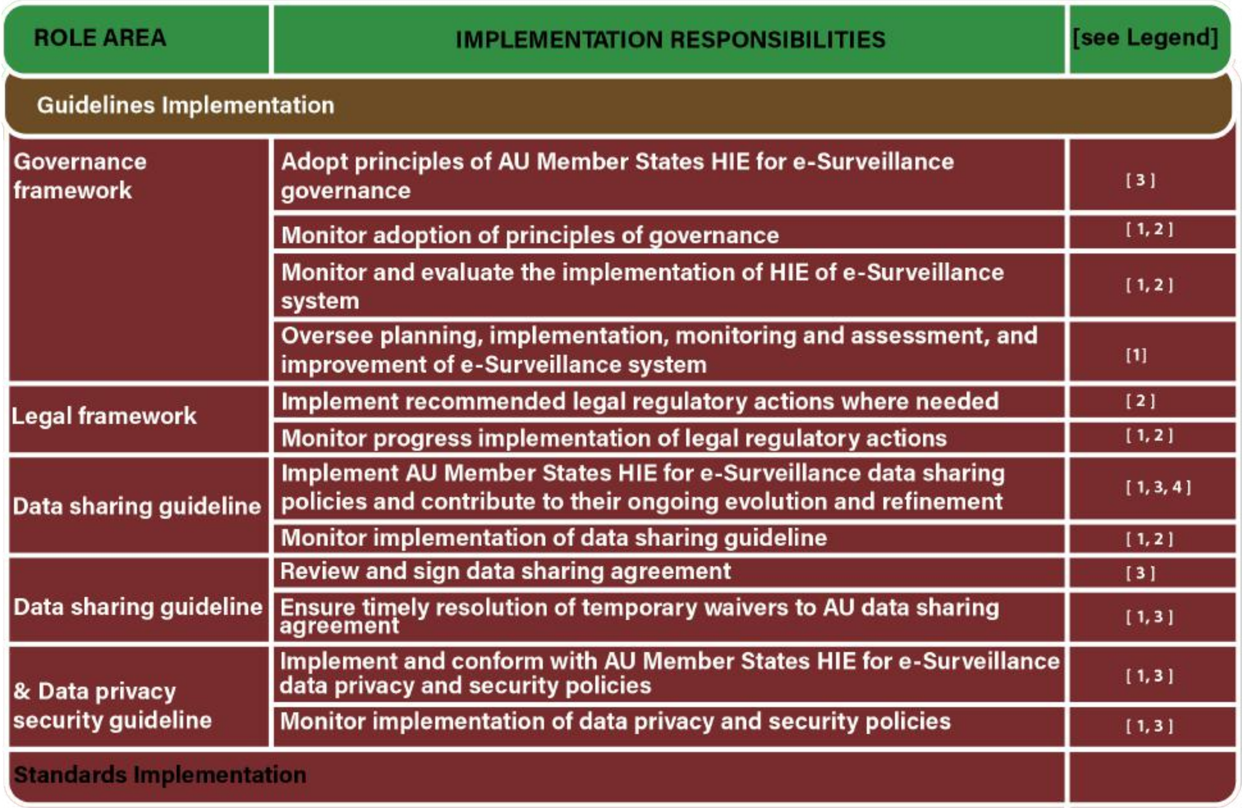
- Data driven decision making through data mining processes.
- Better monitoring and evaluation of public health interventions due to improved data availability and automated analysis tools.

e) Cost management

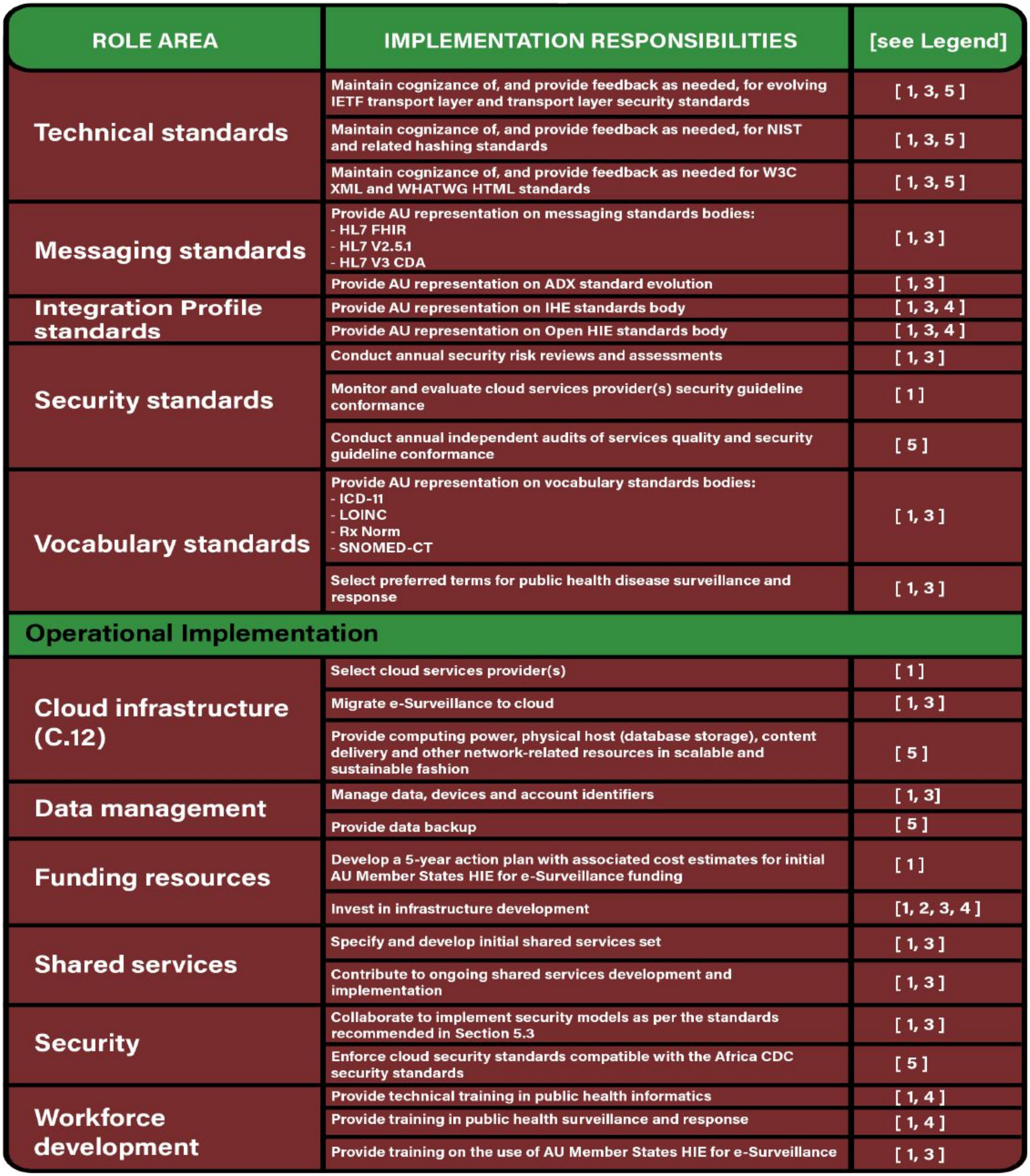
- Reduced costs for management of disease outbreaks.
- Reduced public health costs due to earlier detection of disease outbreaks.

Implementation and sustainment of the AU Member States HIE for e-Surveillance require the engagement and participation of multiple stakeholders. Table 2 below outlines the high-level implementation responsibilities by role area and provides the associated implementation framework.

Table 2. AU Member States HIE for e-Surveillance Role Areas and Responsibilities



ROLE AREA	IMPLEMENTATION RESPONSIBILITIES	[see Legend]
Guidelines Implementation		
Governance framework	Adopt principles of AU Member States HIE for e-Surveillance governance	[3]
	Monitor adoption of principles of governance	[1, 2]
	Monitor and evaluate the implementation of HIE of e-Surveillance system	[1, 2]
	Oversee planning, implementation, monitoring and assessment, and improvement of e-Surveillance system	[1]
Legal framework	Implement recommended legal regulatory actions where needed	[2]
	Monitor progress implementation of legal regulatory actions	[1, 2]
Data sharing guideline	Implement AU Member States HIE for e-Surveillance data sharing policies and contribute to their ongoing evolution and refinement	[1, 3, 4]
	Monitor implementation of data sharing guideline	[1, 2]
Data sharing guideline	Review and sign data sharing agreement	[3]
	Ensure timely resolution of temporary waivers to AU data sharing agreement	[1, 3]
& Data privacy security guideline	Implement and conform with AU Member States HIE for e-Surveillance data privacy and security policies	[1, 3]
	Monitor implementation of data privacy and security policies	[1, 3]
Standards Implementation		



ROLE AREA	IMPLEMENTATION RESPONSIBILITIES	[see Legend]
Technical standards	Maintain cognizance of, and provide feedback as needed, for evolving IETF transport layer and transport layer security standards	[1, 3, 5]
	Maintain cognizance of, and provide feedback as needed, for NIST and related hashing standards	[1, 3, 5]
	Maintain cognizance of, and provide feedback as needed for W3C XML and WHATWG HTML standards	[1, 3, 5]
Messaging standards	Provide AU representation on messaging standards bodies: - HL7 FHIR - HL7 V2.5.1 - HL7 V3 CDA	[1, 3]
	Provide AU representation on ADX standard evolution	[1, 3]
Integration Profile standards	Provide AU representation on IHE standards body	[1, 3, 4]
	Provide AU representation on Open HIE standards body	[1, 3, 4]
Security standards	Conduct annual security risk reviews and assessments	[1, 3]
	Monitor and evaluate cloud services provider(s) security guideline conformance	[1]
	Conduct annual independent audits of services quality and security guideline conformance	[5]
Vocabulary standards	Provide AU representation on vocabulary standards bodies: - ICD-11 - LOINC - Rx Norm - SNOMED-CT	[1, 3]
	Select preferred terms for public health disease surveillance and response	[1, 3]
Operational Implementation		
Cloud infrastructure (C.12)	Select cloud services provider(s)	[1]
	Migrate e-Surveillance to cloud	[1, 3]
	Provide computing power, physical host (database storage), content delivery and other network-related resources in scalable and sustainable fashion	[5]
Data management	Manage data, devices and account identifiers	[1, 3]
	Provide data backup	[5]
Funding resources	Develop a 5-year action plan with associated cost estimates for initial AU Member States HIE for e-Surveillance funding	[1]
	Invest in infrastructure development	[1, 2, 3, 4]
Shared services	Specify and develop initial shared services set	[1, 3]
	Contribute to ongoing shared services development and implementation	[1, 3]
Security	Collaborate to implement security models as per the standards recommended in Section 5.3	[1, 3]
	Enforce cloud security standards compatible with the Africa CDC security standards	[5]
Workforce development	Provide technical training in public health informatics	[1, 4]
	Provide training in public health surveillance and response	[1, 4]
	Provide training on the use of AU Member States HIE for e-Surveillance	[1, 3]

Legend: [1] Africa CDC; [2] AU Member States; [3] AU Member States' NPHIs or equivalent or MOH; [4] Partner(s); [5] Services provider(s)

7. Illustrative AU Member States HIE for e-Surveillance Implementation Use Cases

The following section provides use cases describing how the guidelines and standards provided in Section B can be applied to specific disease domains.

7.1. COVID-19 case-based surveillance

Purpose

This e-Surveillance use case gives a standard way to send COVID-19 case and lab data to the Africa CDC electronically, based on the policies and standards set out in the recommendations of the Africa CDC HIE Task Force.

Implementation

Figure 2 highlights the implementation details required to realize this use case.

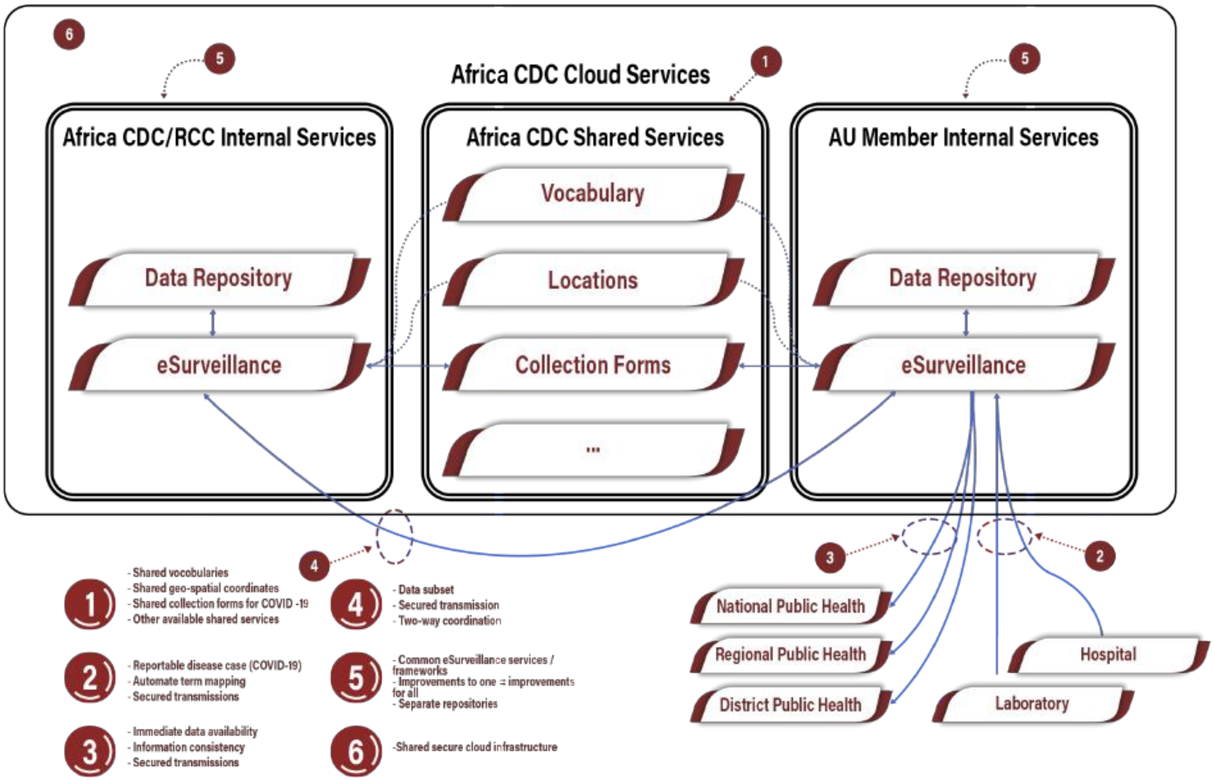

6
5
Africa CDC Cloud Services
1
5
Africa CDC/RCC Internal Services
Africa CDC Shared Services
AU Member Internal Services
Vocabulary
Data Repository
Locations
Data Repository
eSurveillance
Collection Forms
eSurveillance
...
4
3
2
National Public Health
Regional Public Health
Hospital
District Public Health
Laboratory
1
- Shared vocobularies
- Shared geo-spatial coordinates
- Shared collection forms for COVID -19
- Other available shared services
4
- Data subset
- Secured transmission
- Two-way coordination
2
- Reportable disease case (COVID-19)
- Automate term mapping
- Secured transmissions
5
- Common eSurveillance services / frameworks
- Improvements to one = improvements for all
- Separate repositories
3
- Immediate data availability
- Information consistency
- Secured transmissions
6
-Shared secure cloud infrastructure

Figure 2. Implementation for COVID-19 Use Case

The above graphic includes the following elements (as identified by each circled number):

1. Services that are used by all e-Surveillance instances and are hosted by the Africa CDC. The services include Africa CDC-defined standards like preferred terms and codes, a locations registry to support geospatial mapping and display of public health data, previously developed public health data collection forms with embedded vocabulary that can be quickly reused by multiple AU Member States, as well as other shared services and relevant metadata as needed. For this use case, all AU Member e-Surveillance services can easily reuse a single COVID-19 data collection form that is mapped to standard terminologies. The vocabulary service would be made based on what the Africa CDC HIE for e-Surveillance Task Force says should be done.

2. Reporting of reportable diseases directly into the AU Member state's e-Surveillance system from hospital and laboratory sources as per their respective national surveillance reporting guidelines. Source data entry can be via a web-based application using mobile devices and computers. Source terminology would be automatically mapped, and transformed, to the HL7 FHIR messages with associated case documents. All data transmissions would be via a secure network channel to ensure data security and privacy.

3. The Member State's Ministry of Health (MoH) or National Public Health Information System (NPHI) or equivalent, as well as the relevant regional and district public health offices, can see the reported data right away. All levels share the same information, so they all have the same picture of how the COVID-19 pandemic is changing.

4. A subset of reported data is also immediately available to the Africa CDC (based on the data sharing agreement with the AU Member States). Data would be transmitted to the Africa CDC/RCC e-Surveillance service via HL7 FHIR messages with case data and associated documents. All data transmissions would be via a secure network channel. A separate subset of reported data can also immediately be available to the WHO (based on WHO guidance and data use agreements). Data would be transmitted to WHO via appropriate standards-based format. All data transmissions would be via a secure network channel.

5. Common standards-based e-Surveillance digital health solutions residing on different servers to support both the Africa CDC and each AU Member State. Working as a Community of Practice will contribute and share resources, experts, efforts and technology artefacts for the benefits of each AU participant using the e-Surveillance solution. Separate public health data repositories for the Africa CDC and each AU Member state protect national data, but with common defined data elements, element definitions and structures would permit ready sharing and exchange of allowed data sets (both between the AU Member state and the Africa CDC, but also potentially between other AU Members (e.g., alerts to a neighboring Member State of increased incidence of COVID-19 cases along a shared border)).

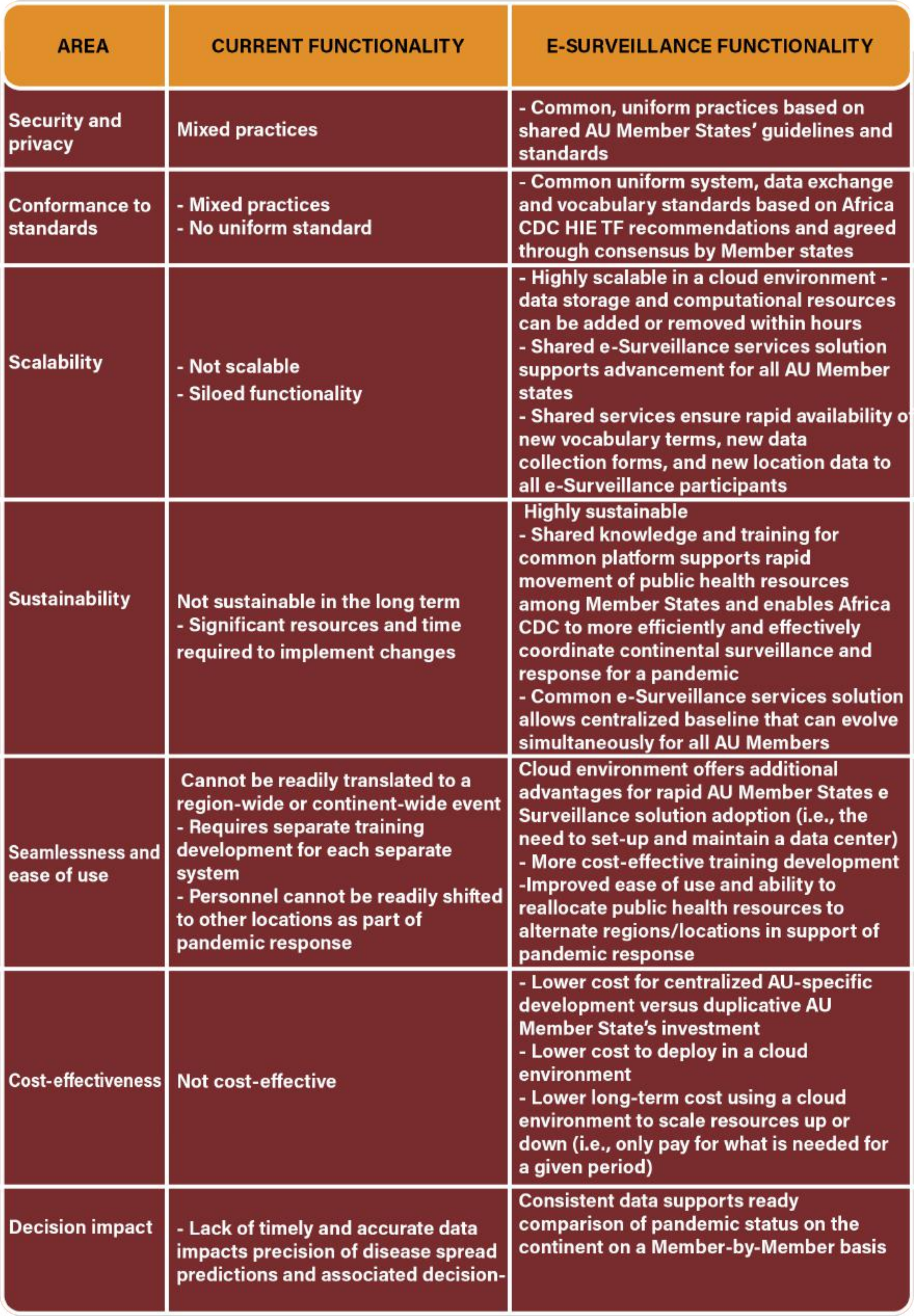
The platform for Africa CDC, AU Member States, and shared parts of this implementation can be either a cloud-services environment (provided by the Africa CDC, the AU, or a third-party cloud-services provider with facilities on the continent; see also Section 9) or data centers that are owned and run separately by the Africa CDC and each Member State. The first scenario cuts costs (for both equipment and resources), makes it easier to share data, and makes it easier to share services and software/system updates. Both of these plans keep national data safe.

For COVID-19 response, reporting from Member States would include the data elements shown in Annexure 6 and 7.

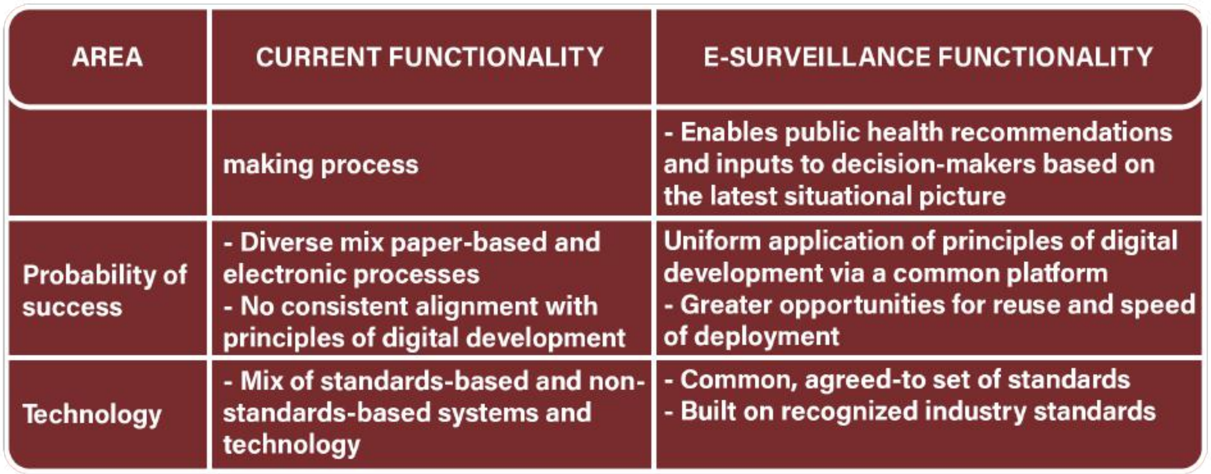
Assessment

Table 3 below provides a comparative assessment between current functionality for integrated disease surveillance and reporting and the proposed COVID-19 e-Surveillance solution.

Table 3. Assessment of e-Surveillance Solution for COVID-19 Response



AREA	CURRENT FUNCTIONALITY	E-SURVEILLANCE FUNCTIONALITY
Security and privacy	Mixed practices	- Common, uniform practices based on shared AU Member States' guidelines and standards
Conformance to standards	- Mixed practices - No uniform standard	- Common uniform system, data exchange and vocabulary standards based on Africa CDC HIE TF recommendations and agreed through consensus by Member states
Scalability	- Not scalable - Siloed functionality	- Highly scalable in a cloud environment - data storage and computational resources can be added or removed within hours - Shared e-Surveillance services solution supports advancement for all AU Member states - Shared services ensure rapid availability o new vocabulary terms, new data collection forms, and new location data to all e-Surveillance participants
Sustainability	Not sustainable in the long term - Significant resources and time required to implement changes	Highly sustainable - Shared knowledge and training for common platform supports rapid movement of public health resources among Member States and enables Africa CDC to more efficiently and effectively coordinate continental surveillance and response for a pandemic - Common e-Surveillance services solution allows centralized baseline that can evolve simultaneously for all AU Members
Seamlessness and ease of use	Cannot be readily translated to a region-wide or continent-wide event - Requires separate training development for each separate system - Personnel cannot be readily shifted to other locations as part of pandemic response	Cloud environment offers additional advantages for rapid AU Member States e Surveillance solution adoption (i.e., the need to set-up and maintain a data center) - More cost-effective training development -Improved ease of use and ability to reallocate public health resources to alternate regions/locations in support of pandemic response
Cost-effectiveness	Not cost-effective	- Lower cost for centralized AU-specific development versus duplicative AU Member State's investment - Lower cost to deploy in a cloud environment - Lower long-term cost using a cloud environment to scale resources up or down (i.e., only pay for what is needed for a given period)
Decision impact	- Lack of timely and accurate data impacts precision of disease spread predictions and associated decision-	Consistent data supports ready comparison of pandemic status on the continent on a Member-by-Member basis



AREA	CURRENT FUNCTIONALITY	E-SURVEILLANCE FUNCTIONALITY
	making process	- Enables public health recommendations and inputs to decision-makers based on the latest situational picture
Probability of success	- Diverse mix paper-based and electronic processes - No consistent alignment with principles of digital development	Uniform application of principles of digital development via a common platform - Greater opportunities for reuse and speed of deployment
Technology	- Mix of standards-based and non-standards-based systems and technology	- Common, agreed-to set of standards - Built on recognized industry standards

7.2. HIV case-based surveillance

Purpose

This e-Surveillance use case provides a standard method to electronically send HIV case and lab data to Africa CDC based on enabling policies and standards specified in the Africa CDC HIE Task Force recommendations.

Reportable data flow

Africa CDC would use the HIE for e-Surveillance solution to support direct reporting of HIV case-based data from Member States to Africa CDC RCCs or directly to Africa CDC for future operations on the continent. Every new HIV case would be reported right away if a patient's lab test came back positive. As antiretroviral therapy (ART) drugs are given out, compliance with HIV treatment plans would also be reported. The HIE for e-Surveillance solution would make it easier for Member States and reporting entities (like hospitals and labs) in the region to collect detailed data (i.e., via mobile device or computer through secure message transmission channels), as well as collect more types of data. With the HIE for e-Surveillance solution, the Africa CDC would be able to collect aggregated, pre-defined indicator-based data from AU Member States in an automated way. As the continental HIV response changes and moves toward HIV suppression in the African population, the subset of case-based indicators will also change to best support the continental HIV response (e.g., more detail on case demographics, loss-to-follow-up, deaths where HIV/AIDS is the main cause or a contributing comorbidity, etc.). The solution can also directly connect to lab testing devices and hospital electronic medical record systems that can share data. This speeds up reporting within Member States.

Implementation

Implementation of this use case will be similar to the implementation provided for the COVID-19 use case. For the Member States, their e-Surveillance instance will track HIV case-based data, providing a richer data set for query and analysis, and for extraction of aggregated data sets as needed by the Africa CDC. The primary differences will be:

a) Differences in reported data elements (e.g., ART initiation; ART medication pick-ups; mother-to-child transmission prevention treatments) (see also Annexure 2).
b) Differences in vocabulary terms (e.g., for HIV recency and CD4 test results; for the inclusion of tuberculosis and sexually transmitted disease data)
c) Use of ADX standard for exchange of aggregated data between the Member State e-Surveillance systems and the Africa CDC e-Surveillance instance.
d) Opportunities for consolidation of reporting to external partners.

Assessment

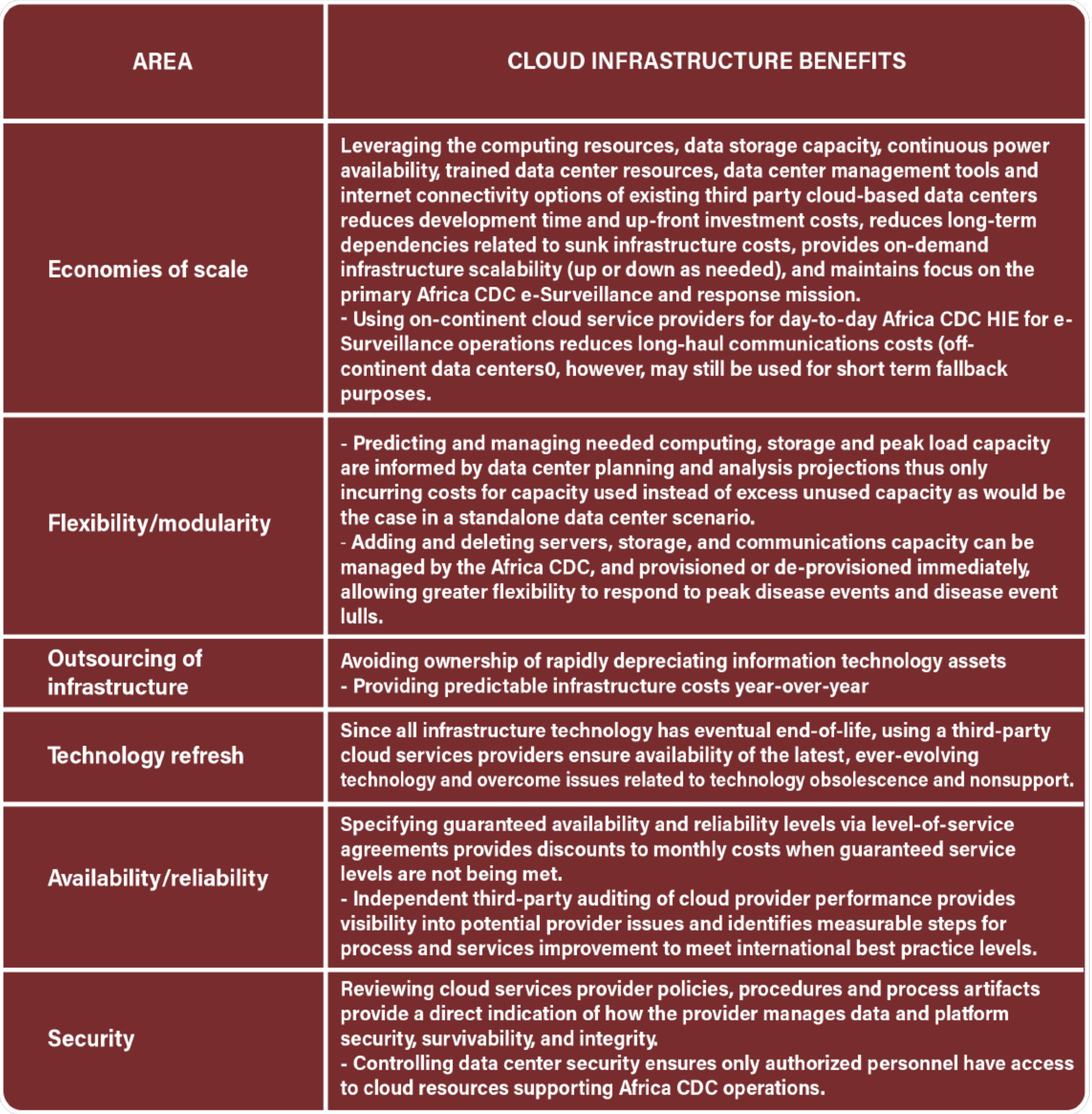
For the HIV case-based surveillance use case, the assessment of current functionality vs. HIE for e-Surveillance functionality is similar to what was done for the COVID-19 use case in the previous section. The HIE for e-Surveillance can also be used for activities related to managing chronic diseases.

7.3. Cloud and shared services

Recommended models

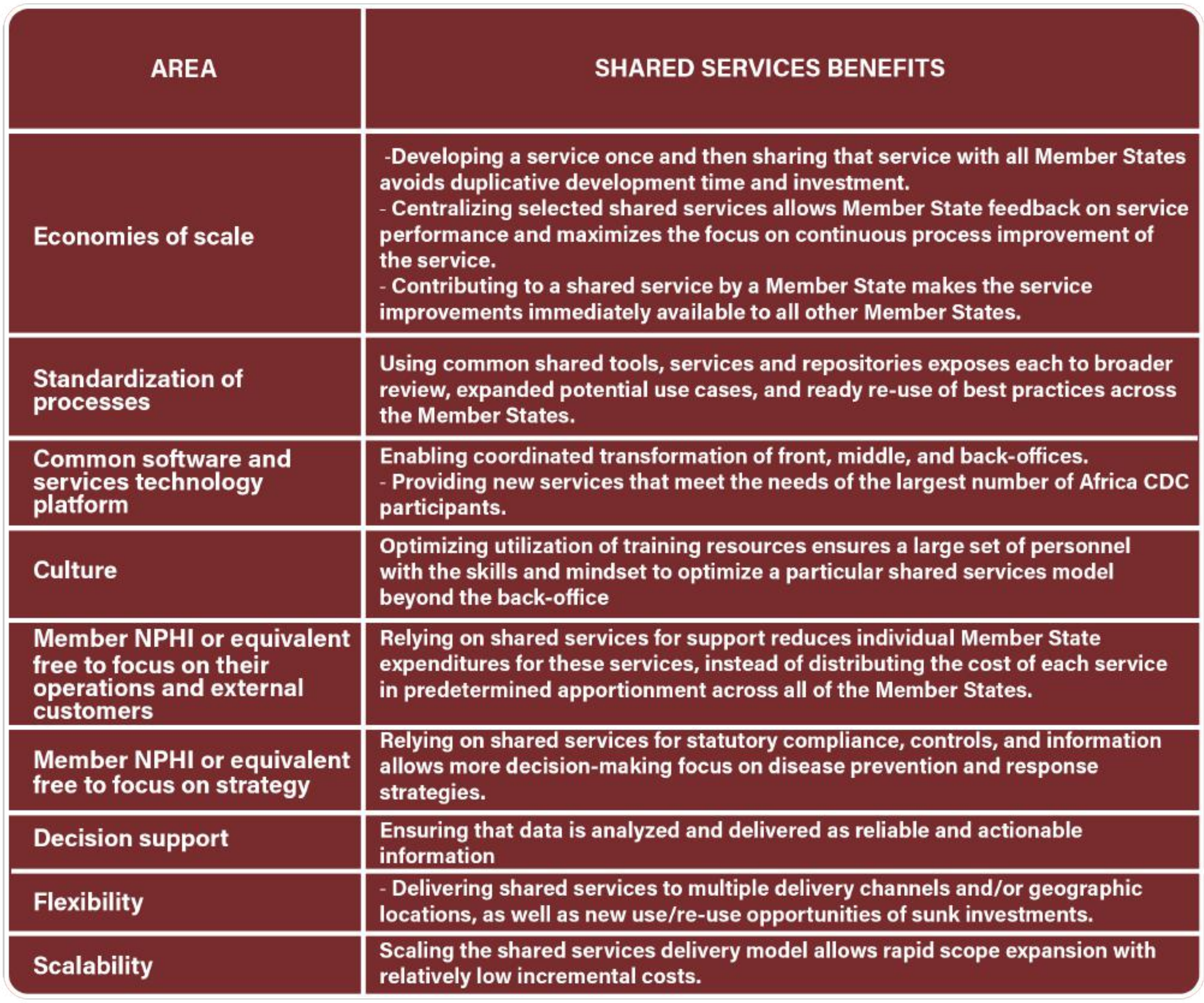
The benefits of cloud and shared services for HIE for e-Surveillance implementation and deployment are described in Tables 4 and 5 below.

Table 4. Cloud Infrastructure Benefits for AU Member States HIE for e-Surveillance.



AREA	CLOUD INFRASTRUCTURE BENEFITS
Economies of scale	Leveraging the computing resources, data storage capacity, continuous power availability, trained data center resources, data center management tools and internet connectivity options of existing third party cloud-based data centers reduces development time and up-front investment costs, reduces long-term dependencies related to sunk infrastructure costs, provides on-demand infrastructure scalability (up or down as needed), and maintains focus on the primary Africa CDC e-Surveillance and response mission. - Using on-continent cloud service providers for day-to-day Africa CDC HIE for e-Surveillance operations reduces long-haul communications costs (off-continent data centers0, however, may still be used for short term fallback purposes.
Flexibility/modularity	- Predicting and managing needed computing, storage and peak load capacity are informed by data center planning and analysis projections thus only incurring costs for capacity used instead of excess unused capacity as would be the case in a standalone data center scenario. - Adding and deleting servers, storage, and communications capacity can be managed by the Africa CDC, and provisioned or de-provisioned immediately, allowing greater flexibility to respond to peak disease events and disease event lulls.
Outsourcing of infrastructure	Avoiding ownership of rapidly depreciating information technology assets - Providing predictable infrastructure costs year-over-year
Technology refresh	Since all infrastructure technology has eventual end-of-life, using a third-party cloud services providers ensure availability of the latest, ever-evolving technology and overcome issues related to technology obsolescence and nonsupport.
Availability/reliability	Specifying guaranteed availability and reliability levels via level-of-service agreements provides discounts to monthly costs when guaranteed service levels are not being met. - Independent third-party auditing of cloud provider performance provides visibility into potential provider issues and identifies measurable steps for process and services improvement to meet international best practice levels.
Security	Reviewing cloud services provider policies, procedures and process artifacts provide a direct indication of how the provider manages data and platform security, survivability, and integrity. - Controlling data center security ensures only authorized personnel have access to cloud resources supporting Africa CDC operations.

Table 5. Shared Services Benefits for HIE for e-Surveillance.



AREA	SHARED SERVICES BENEFITS
Economies of scale	-Developing a service once and then sharing that service with all Member States avoids duplicative development time and investment. - Centralizing selected shared services allows Member State feedback on service performance and maximizes the focus on continuous process improvement of the service. - Contributing to a shared service by a Member State makes the service improvements immediately available to all other Member States.
Standardization of processes	Using common shared tools, services and repositories exposes each to broader review, expanded potential use cases, and ready re-use of best practices across the Member States.
Common software and services technology platform	Enabling coordinated transformation of front, middle, and back-offices. - Providing new services that meet the needs of the largest number of Africa CDC participants.
Culture	Optimizing utilization of training resources ensures a large set of personnel with the skills and mindset to optimize a particular shared services model beyond the back-office
Member NPHI or equivalent free to focus on their operations and external customers	Relying on shared services for support reduces individual Member State expenditures for these services, instead of distributing the cost of each service in predetermined apportionment across all of the Member States.
Member NPHI or equivalent free to focus on strategy	Relying on shared services for statutory compliance, controls, and information allows more decision-making focus on disease prevention and response strategies.
Decision support	Ensuring that data is analyzed and delivered as reliable and actionable information
Flexibility	- Delivering shared services to multiple delivery channels and/or geographic locations, as well as new use/re-use opportunities of sunk investments.
Scalability	Scaling the shared services delivery model allows rapid scope expansion with relatively low incremental costs.

To realize continental surveillance connectivity, Africa CDC will provide a secure and interoperable cloud-based e-Surveillance platform, Software as a Service (SaaS) and Mobile backend as a Service (MBaaS) that centralizes and shares common IT services needed for disease surveillance. Additionally, the Africa CDC & African Union to help build similar Cloud and shared services across Member States for easy accessibility to data.

Within the context of the Africa CDC HIE for e-Surveillance, the implementation of the cloud computing model shall take one of the following forms:

a) **Africa CDC cloud infrastructure** - owned, managed, and operated by Africa CDC, and provisioned for exclusive use by the Africa CDC and AU Member States for HIE for e-Surveillance to achieve shared policies and requirements. This aligns with the *Statute of the Africa Centers for Disease Control and Prevention (Africa CDC)* which states that Africa CDC is an Africa-owned institution with the Member States maintaining national-level ownership of the Africa CDC simultaneously, both as advisors and through direct programmatic engagement. This represents the most expedient model for implementation as it would be entirely under Africa CDC control.

b) **AU cloud infrastructure** - owned, managed, and operated by the AU, and provisioned to support a range of computing, networking and services needs within the African continent for itself and its Member States, including HIE for e-Surveillance for Africa CDC and Member State NPHIs or equivalent. This model may not be as expedient as a private cloud approach since it does require buy-in from the AU Member States. However, adoption of this model may encourage AU Members to accelerate their use of the shared services and tools, as well as the integration of other digital health and m-Health services exclusively for Member use.

c) **Hybrid cloud infrastructure** - a combination of the above cloud infrastructures bound together by standardized technology to enable data and application portability (e.g., load balancing between clouds). The use of (at least) two clouds offers the ability to strategically split operational considerations between two separate providers (e.g., Africa CDC cloud to provide day-to-day operational HIE for e-Surveillance services and AU cloud to backup HIE for e-Surveillance data) providing risk reduction in the event a provider becomes non-viable at some point in the future.

Of these three, the Africa CDC recommends adoption of the Africa CDC cloud infrastructure model in the immediate near-term and that the AU provides its own continental AU cloud infrastructure model to support the above hybrid cloud infrastructure model in the long-term. The prerequisites of successful implementation of the cloud-based infrastructure and services are shown in Annexure 9.

Requisite shared services

The AU Member States HIE for e-Surveillance shall provide the following shared repository services at a minimum:

a) **Unique entity identifier management and matching service -** provide a digital unique patient identifier for each patient across applications in the continent. This service facilitates the access of accurate and current demographic and essential medical patient data from databases in the AU Member States. The profile integration and mapping standards recommended in Section 4.5 will be implemented here. This will provide data and tools to rapidly associate new data with previously reported data to prevent duplication of reportable disease counts (e.g., number tested, number infected, number treated, number recovered, number died, number lost to follow-up, etc.), and ensure consistent reporting for disease response planning, decision-making, and efficacy. Africa CDC will not receive actual identifiers from the Member States but use this internal service.

b) **Location geospatial data service** - provides data and tools to associate a place name (e.g., province, city, hospital, clinic) with its associated geospatial coordinates, or with a geospatial entity (e.g., a shape file) to support the use of mapping tools for location-based disease surveillance, tracking and response status reporting.

c) **Vocabulary service** - provides data and tools to identify the preferred set of vocabulary terms and concepts associated with specific disease reporting to ensure consistency of reporting from Member States NPHIs or equivalent and to speed Africa CDC disease progression analysis. This may also include mapping between these preferred terms and equivalent terms to facilitate automated message processing and transformation into the preferred nomenclature for data analysis. This will foster disease surveillance interoperability among heterogeneous platforms. Common disease surveillance terminology and nomenclature will be used, as mentioned in Section 4.4, across the Continent to securely share disease surveillance information using the cloud-based infrastructure.

d) **Data collection form sharing service** - provide data and tools to define data collection forms, data elements, and associated vocabularies for specific disease reporting for re-use by the Member States to facilitate public health data exchange and speed dissemination of data collection guidance to all Member State NPHIs or equivalent.

The AU Member States HIE for e-Surveillance shall provide the following application services at a minimum:

a) **E-Surveillance [data entry]** - provide tools to manage reportable data entry from Member State laboratories and hospitals.

b) **E-Surveillance [data retrieval & display]** - provide tools to alert national, regional and district public health authorities to the availability of new data and to access and display available data with appropriate controls on data visibility at each level. Similarly, provide tools to alert the Africa CDC and associated RCC to the availability of new data released by a Member State National public health authority and to access and display the available data with appropriate controls on data visibility.

c) **E-Surveillance [data release]** - provide tools to affect the release and transfer of new data to the Africa CDC and associated RCC for processing. Similarly, provide tools to affect the release and transfer of Africa CDC data to the WHO.

d) **E-Surveillance [coordination]** - provide tools to allow Africa CDC and Member State national public health authorities to collaborate on shared data and response plans.

e) **E-Surveillance [decision making and data visualization service]** - provide the decision support tools for data analytics, data visualization, information dissemination, disease forecasting, real-time detection of epidemics, public health alert services, and re-usable disease dashboard components to facilitate the assessment of current disease surveillance and response status.

The AU Member States HIE for e-Surveillance shall provide the following data repository services at a minimum:

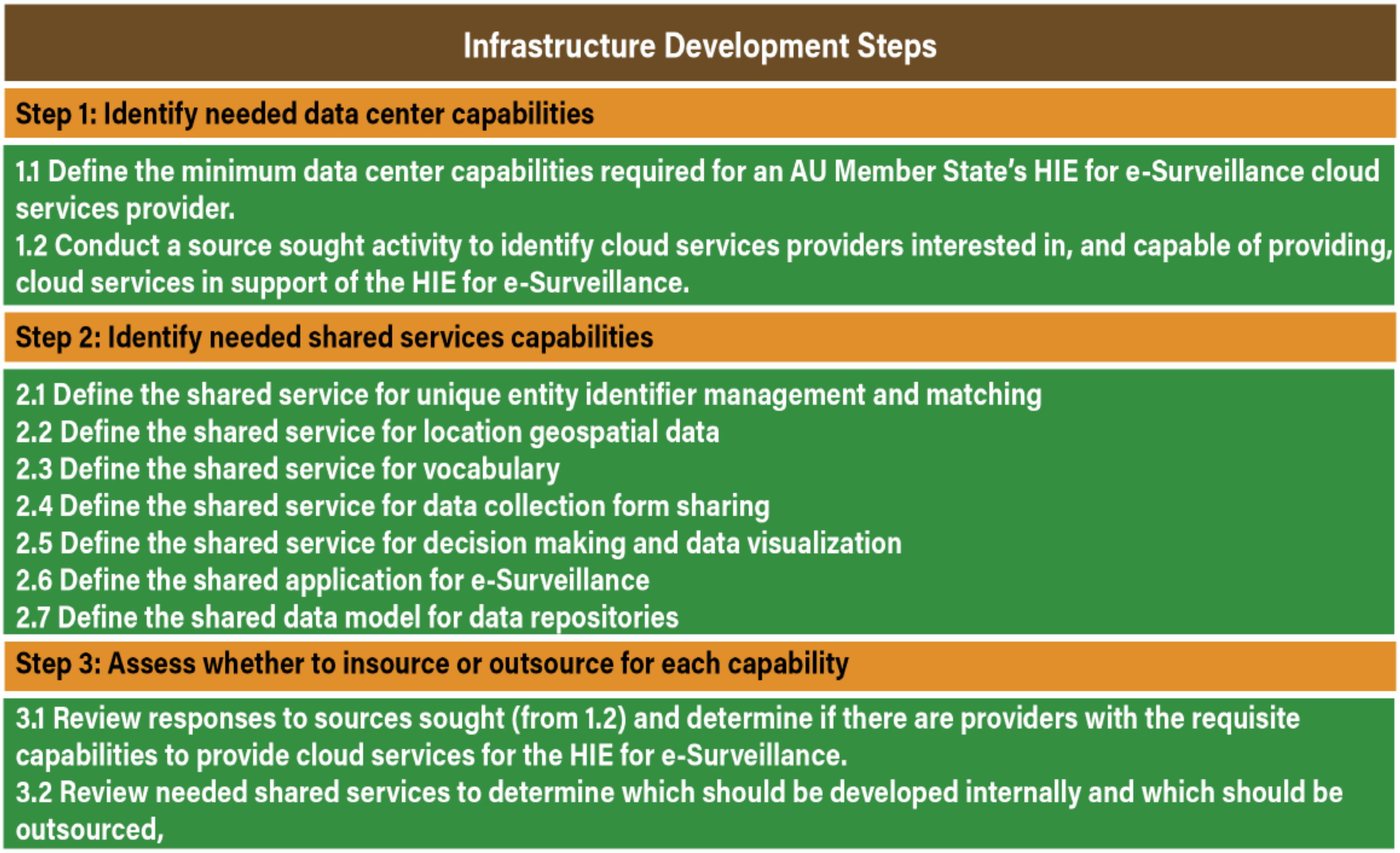
a) **Data repository** - provide Africa CDC/RCCs and each Member State with a separate data repository for any and all data under their control.

Each of the above service sets will be created by the Africa CDC either on its own or with help from a third party. The HIE for e-Surveillance will get more shared services over time, based on what the Africa CDC and Member States say and how they plan to improve the process.

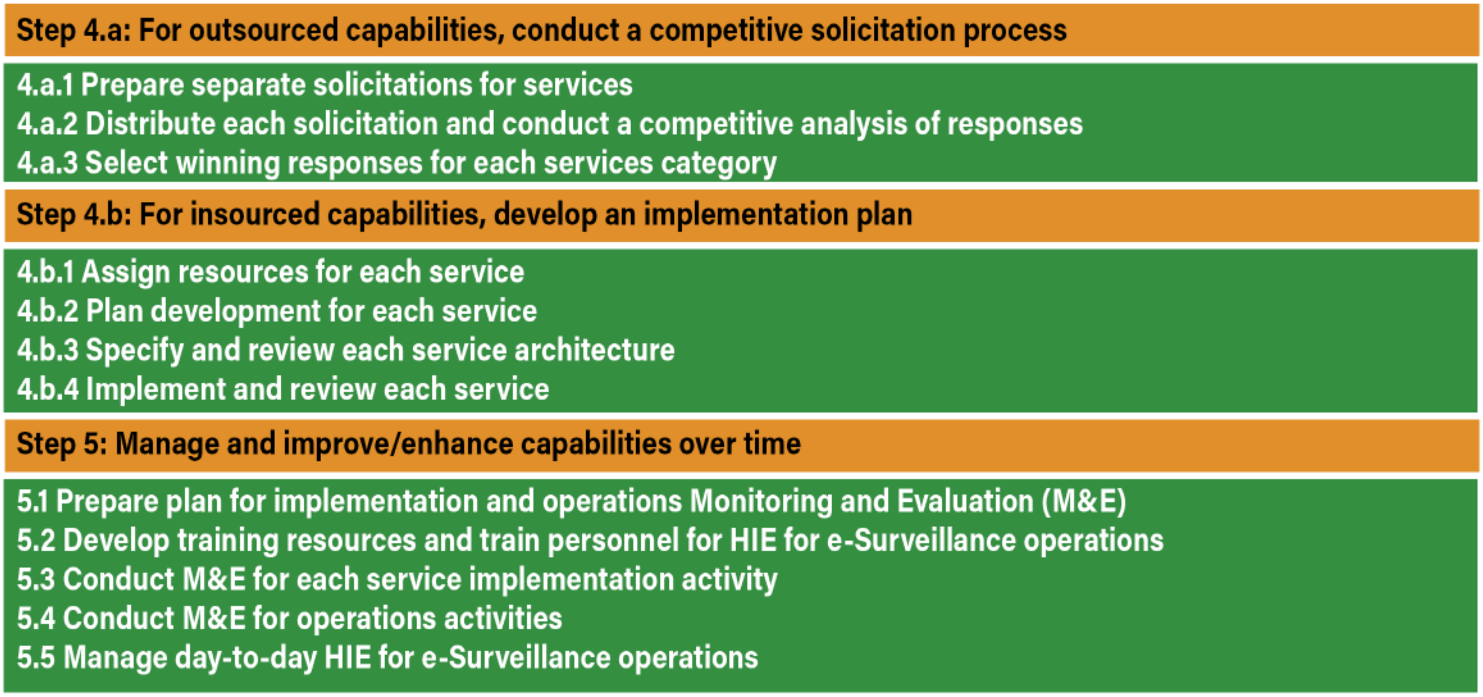
8. Infrastructure Development

Infrastructure consists of hardware, software, people and processes. This section defines the necessary resources to achieve the initial cloud-based / shared-services model for the Africa CDC HIE for e-Surveillance.

Table 6. Infrastructure Development Steps



Infrastructure Development Steps
Step 1: Identify needed data center capabilities
1.1 Define the minimum data center capabilities required for an AU Member State's HIE for e-Surveillance cloud services provider. 1.2 Conduct a source sought activity to identify cloud services providers interested in, and capable of providing, cloud services in support of the HIE for e-Surveillance.
Step 2: Identify needed shared services capabilities
2.1 Define the shared service for unique entity identifier management and matching 2.2 Define the shared service for location geospatial data 2.3 Define the shared service for vocabulary 2.4 Define the shared service for data collection form sharing 2.5 Define the shared service for decision making and data visualization 2.6 Define the shared application for e-Surveillance 2.7 Define the shared data model for data repositories
Step 3: Assess whether to insource or outsource for each capability
3.1 Review responses to sources sought (from 1.2) and determine if there are providers with the requisite capabilities to provide cloud services for the HIE for e-Surveillance. 3.2 Review needed shared services to determine which should be developed internally and which should be outsourced,



Step 4.a: For outsourced capabilities, conduct a competitive solicitation process

4.a.1 Prepare separate solicitations for services
4.a.2 Distribute each solicitation and conduct a competitive analysis of responses
4.a.3 Select winning responses for each services category

Step 4.b: For insourced capabilities, develop an implementation plan

4.b.1 Assign resources for each service
4.b.2 Plan development for each service
4.b.3 Specify and review each service architecture
4.b.4 Implement and review each service

Step 5: Manage and improve/enhance capabilities over time

5.1 Prepare plan for implementation and operations Monitoring and Evaluation (M&E)
5.2 Develop training resources and train personnel for HIE for e-Surveillance operations
5.3 Conduct M&E for each service implementation activity
5.4 Conduct M&E for operations activities
5.5 Manage day-to-day HIE for e-Surveillance operations

9. Capacity Building

Africa CDC and the AU Member States shall provide the necessary resources to support the AU Member States HIE for digital health system to include:

a) Acquisition and procurement of system infrastructure.
b) Acquisition and procurement of system cloud platform(s).
c) Development of disease-based use cases for public health to include messaging exchange formats, message content, and associated vocabularies.
d) Design and development of shared registries.
e) Architecture, development and integration of common digital health system tools.
f) Ongoing audit of HIE for digital health system information privacy and security.
g) Ongoing review and audit of the HIE for digital health system infrastructure and cloud platform(s).
h) Participation and coordination with standards and partner organizations.
i) Provide both short-term and long-term internships for bachelors, masters and PhD level informatics and health science students from the continent.

j) Develop a curriculum on health informatics and epidemiology fellowship to train a cadre of competent health informatics and data science experts that can be deployed to AU member states.

k) Develop a framework/plan to foster private sector engagement for long term sustainability of the digital health system.

10. Investment

Developing a health system and investing in digital health are becoming a priority in AU Member States. Over the past decade, AU Member States have invested significantly in digital health interventions; however, informed investment decisions towards HIE for digital health systems lack. To have an HIE for digital health systems among AU Member States, an investment profile that includes a national EHR that supports nationa, regional, and continental HIE, a National HIS and data warehouse, a patient portal, and registers (populations) is required. The following principles can be followed to invest in HIE for digital health systems among AU Member States:

- **Whole-of-government approach:** investment for HIE of digital health systems among AU Member States shall follow a whole-of-government approach to develop and implement a sustainable HIE platform. This approach can deliver reusable digital services at scale with a greater return on investment [52].
- **Cooperative investment approach**: this approach invites customers, AU Member States, health care providers and health professionals, partners, private sector, providers of digital health software, hardware and services shall come together to invest in HIE among digital health systems [53].
- **Investment case framework:** to invest in HIE for digital health systems, understanding of the inputs, processes, outputs, and benefits is needed. The Global Financing Facility [54] has suggested an approach to develop an investment case framework that will support the required investment. This framework, as shown in Figure 3, shall be adopted by AU Member States for successful implementation of HIE for digital health Systems.

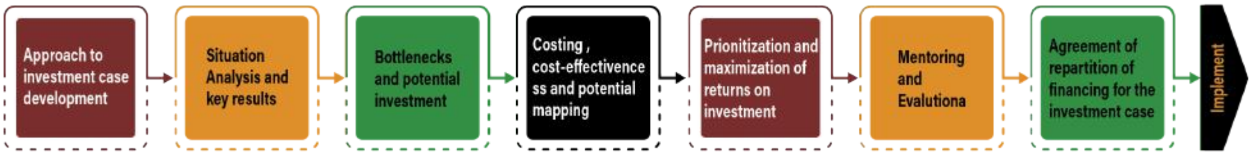

Approach to investment case development
Situation Analysis and key results
Bottlenecks and potential investment
Costing , cost-effectivence ss and potential mapping
Prionitization and maximization of returns on investment
Mentoring and Evalutiona
Agreement of repartition of financing for the investment case
Implement

Figure 3: Investment framework of HIE for digital health systems of AU Member States. Source: Global Financing Facility [54].

- **Digital Framework Investment Review Tool:** the AU Member States shall use the Digital Framework Investment Review Tool that is developed by Measure Evaluation [55]. The tool provides high-level guidance based on widely-accepted best practices such as the principle for Digital Development and Donor Investment Principles that can be used to support strategic investment in the use of digital technologies to support public and global health.

11. Monitoring, Evaluation and Research

The purposes of monitoring, evaluation and research include:

- Monitoring progress towards the implementation of the AU HIE guidelines and standards,
- Identifying critical differences between planned and actual implementation,
- Identifying barriers to and facilitators of implementation,
- Identifying and forwarding future priorities by undertaking scientific research

Monitoring shall include continuous manual and automated assessment of HIE for digital health system implementation, deployment, adoption and use. The evaluation shall include an examination of the HIE for digital health system relevance, effectiveness, efficiency and impact in terms of Africa CDC's evolving goals and objectives. Specific M&E actions for the HIE for digital health system infrastructure shall include:

a) Annual survey of HIE for digital health system users and support personnel to determine satisfaction levels, the services that are working as intended, the services that are not working as intended, and potential areas for improvement.

b) Initial on-site visit to cloud services providers to review policies, procedures and existing procedure artifacts; evaluate data center security status; observe data center operations; and establish baseline assessment and any provider change recommendations.

c) Annual review of the independent audit report(s) for cloud services providers. Such independent audits shall be conducted in accordance with accepted international auditing standards (e.g., IAES 3402, SAEC 16, etc.).

d) Annual assessment of cloud services provider performance and development of recommendations for service improvements and/or alternate cloud services options.

e) Annual test of cloud services provider data fail-over and recovery processes and review of response times, the potential for services disruptions, and recommendations for improvement.

f) Tracking all actions taken to implement each M&E recommendation.

Specific M&E actions for the HIE for digital health system adoption and use shall include:

a) Measurement and tracking Member State participation in, and adoption of the best practices promulgated by, the ANPHI.

b) Member State use of the HIE for digital health systems.

c) Member State progress towards alignment with, and maturity in, the achievement of the policies, regulations and standards detailed in Sections A and B.

d) Tracking membership and participation in messaging and vocabulary standards bodies.

Specific M&E actions for the HIE for digital health systems operations shall include:

a) Ongoing assessment of data quality improvement from each Member State.

b) Completion and effective use of HIE for digital health workforce training resources.

c) Ongoing assessment of relative workloads, response times, and decision-making quality based on the adoption of the HIE for digital health over time.

d) Assessment of pilot implementations of the HIE for digital health and recommendations for improvement prior to full deployment.

e) Use of cloud management and monitoring tools to assess the use, performance, and health of the cloud services, applications, infrastructure, and workloads.

For successful implementation of HIE guidelines and standards for digital health systems, the Member States shall work together with national universities, research institutes, and partners to:

a) Conduct an initial investigation on the capability of Member States in terms of human resource, infrastructure, and finance to successfully implement HIE guidelines and standards for digital health systems.
b) Conduct a periodic assessment on the implementation of HIE guidelines and standards for digital health systems.
c) Undertake a scientific research to identify facilitators of and barriers to the implementation of HIE guidelines and standards for digital health systems.
d) Conduct scientific review and research to identify and forward future priorities.
e) Conduct high quality research to determine the impact of HIE guidelines and standards implementation on health service delivery improvements.

For initial and periodic assessments of the implementation of HIE for digital health systems, the "Health Information Systems Interoperability Maturity Toolkit" can be used [56]. The toolkit considers critical factors to successful implementation HIE. The kit includes three main parts: a maturity model, an assessment tool, and a users' guide. The users' guide has a French version which makes it easier to use the toolkit among French-speaking Member States. The HIE maturity model is based on three domains: leadership and governance; human resources; and technology. Each domain has subdomains, for a total of 18 subdomains.

The assessment tool can be used to determine the maturity level of Member States in relation to health data exchange starting from facility level to Africa CDC, WHO, African regional bodies (RCC and REC), partners, and other Member States, as described in the continental HIE architecture. The assessment can be conducted before and after the implementation of the AU HIE guidelines and standards for digital health systems.

References

1. Africa CDC, *Africa CDC Strategic Plan*. 2017: Addis Ababa. p. 57.
2. African Union, *African Union Convention on Cyber Security and Personal Data Protection*, A. Union, Editor. 2014, African Union. p. 37.
3. Lovells, H., *Overview of data protection laws in Africa*, lexology, Editor. 2019, Lexology.
4. Information Regulator South Africa, *Protection of Personal Information Act, 2013*, in *4*, I.R.S. Africa, Editor. 2013, Information Regulator South Africa,: South Africa. p. 156.
5. Otto, M., *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR)*, in *International and European Labour Law: Article-by-Article Commentary*, E. Ales, et al., Editors. 2018, Nomos Verlagsgesellschaft mbH & Co. KG: Baden-Baden. p. 958-981.
6. Kish, L.J. and E.J. Topol, *Unpatients—why patients should own their medical data.* Nature Biotechnology 2015. **33**(2015): p. 921–924.
7. Ballantyne, A., *How should we think about clinical data ownership?* 2020. **46**(5): p. 289-294.
8. Kostkova, P., et al., *Who Owns the Data? Open Data for Healthcare.* 2016. **4**(7).
9. University of Pittsburgh. *Data Use Agreements*. 2020 [cited 2020 17/05/2020]; Available from: https://www.osp.pitt.edu/ccc-data-use-agreements.
10. Stanford University. *Data Use Agreement (DUA) FAQs*. 2020 [cited 2020 17/05/2020]; Available from: https://privacy.stanford.edu/other-resources/data-use-agreement-dua-faqs.
11. Dixon, B.E., et al., *A vision for the systematic monitoring and improvement of the quality of electronic health data.* Stud Health Technol Inform, 2013. **192**: p. 884-8.
12. Dixon, B.E., et al., *Extending an open-source tool to measure data quality: case report on Observational Health Data Science and Informatics (OHDSI).* BMJ Health Care Inform, 2020. **27**(1).
13. Open Knowledge Foundation. *What is Open Data?* 2020 [cited 2020 17/05/2020]; Available from: https://opendatahandbook.org/guide/en/what-is-open-data/#menu.
14. Demski, H., S. Garde, and C. Hildebrand, *Open data models for smart health interconnected applications: the example of openEHR.* BMC Med Inform Decis Mak, 2016. **16**(1): p. 137.
15. Wilkinson, M.D., et al., *The FAIR Guiding Principles for scientific data management and stewardship.* Scientific Data, 2016. **3**(1): p. 160018.
16. Mons, B., et al., *Cloudy, increasingly FAIR; revisiting the FAIR Data guiding principles for the European Open Science Cloud.* Information Services & Use, 2017. **37**: p. 49-56.
17. Waithira, N., B. Mutinda, and P.Y. Cheah, *Data management and sharing policy: the first step towards promoting data sharing.* BMC Med, 2019. **17**(1): p. 80.
18. Sunlight Foundation, *Guidelines for Open Data Policies*. 3 ed. 2014, Washington, USA: Sunlight Foundation. 13.
19. Office of the Information Commissioner Queensland. *Open Data Policy*. 2013 [cited 2020 17/05/2020]; Available from: https://www.oic.qld.gov.au/publications/policies/open-data-policy.
20. Centre on Global Health Security, *A Guide to Sharing the Data and Benefits of Public Health Surveillance*. 2017, London, UK: The Royal Institute of International Affairs Chatham House 40.
21. Emerson, C., et al., *World Data System (WDS) Data Sharing Principles*. 2015, Zenodo: Geneva, Switzerland. p. 1.
22. Research Data Alliance, *Data Sharing Principles in Developing Countries*, in *RDA at Open Data SSDC International Workshop*. 2014, Research Data Alliance: Nairobi, Kenya.
23. The University of Chicago. *Data-sharing Agreements*. 2011 [cited 2020 17/05/2020]; Available from: https://ura.uchicago.edu/page/data-sharing-agreements.

24. Labuschaigne, M., et al., *Protecting participants in health research: The South African Material Transfer Agreement*. 2019. Vol. 109. 2019.
25. Ayatollahi, H. and G. Shagerdi, *Information Security Risk Assessment in Hospitals.* Open Med Inform J, 2017. **11**: p. 37-43.
26. Thieme, E., *Privacy, Security and Confidentiality: Towards Trus*, E.D. Brian, Editor. 2016, Academic Press.
27. Zagar, T.R., et al., *Environmental Scan for the Development of Africa CDC Standards for Electronic Public Health Disease Surveillance*. 2020.
28. Lauren Wu, P.B.T.C., *Recommendations for a Global Framework to Support Health Information Exchange in Low- and Middle-Income Countries*. 2016.
29. Kabaso, B. and M. Korpela. *Architecture for Health Information Systems Interoperability in Africa*. in *8thHealth Informatics in Africa Conference (HELINA 2013)*. 2013. Eldoret, Kenya: Koegni eHealth, Innovation for Development e.V. Germany.
30. South African National Department of Health, *National Health Normative Standards Framework for Interoperability in eHealth in South Africa*, in *240075*. 2014, CSIR and NDoH: Pretoria, South Africa. p. 381.
31. World Health Organization, *Fifty-eight World Health Assembly: Resolutions and Decisions*. 2005, WHO: Geneva, Switzerland. p. 159.
32. World Health Organization, *Sixty-six World Health Assembly: Report of the Executive Board on its 131st and 132nd sessions* 2013, WHO: Geneva, Switzerland. p. 6.
33. World Health Organization, *Seventy-first World Health Assembly: Use of appropriate digital technologies for public health (mHealth)*. 2018, WHO: Geneva, Switzerland. p. 5.
34. World Health Organization, *Seventy-first World Health Assembly: Third report of Committee A*. 2018, WHO: Geneva, Switzerland. p. 8.
35. Ministry of Health Ghana, *Ghana e-Health Strategy*. 2010: Accra, Ghana. p. 80.
36. Ministry of Health and Social Welfare, *The National Digital Health Strategy 2019 – 2024*. 2019: Dar es Salaam, Tanzania. p. 62.
37. Ministry of Health of Kenya, *Kenya National eHealth Policy 2016 – 2030*. 2016: Nairobi, Kenya. p. 64.
38. Ministry of Health of Rwanda, *National Digital Health Strategic Plan 2018-2023*. 2018: Kigali, Rwanda. p. 67.
39. Ministry of Health of Ethiopia, *Ethiopia eHealth Architecture* 2017: Addis Ababa, Ethiopia. p. 29.
40. Oluwaseyi, A., et al., *Health Information Exchange Model for Nigerian Health Information System.* International Journal of Computer Science and Information Security, 2019. **17**(2): p. 181-203.
41. Institute of Medicine Committee on Data Standards for Patient, S., *Patient Safety: Achieving a New Standard for Care* in *Patient Safety: Achieving a New Standard for Care*, P. Aspden, et al., Editors. 2004, National Academies Press (US): Washington (DC). p. 550.
42. Bourquard, K., F. Le Gall, and P. Cousin, *Standards for Interoperability in Digital Health: Selection and Implementation in an eHealth Project*, in *Requirements Engineering for Digital Health*, S.A. Fricker, C. Thümmler, and A. Gavras, Editors. 2015, Springer International Publishing: Cham. p. 95-115.
43. Schulz, S., R. Stegwee, and C. Chronaki, *Standards in Healthcare Data*, in *Fundamentals of Clinical Data Science*, P. Kubben, M. Dumontier, and A. Dekker, Editors. 2019, Springer International Publishing: Cham. p. 19-36.
44. Stroetmann, K., *Digital Health Ecosystem for African Countries: A Guide for Public and Private Actors for establishing Holistic Digital Health Ecosystems in Africa*. 2018, Bonn, Germany: Druckriegel GmbH, Frankfurt am Main.

45. World Health Organization, *Global Diffusion of eHealth: Making Universal Health Coverage Achievable*. Report of the Third Global Survey on eHealth. 2016, Geneva, Switzerland: WHO.
46. Adebesin, F., et al., *A review of interoperability standards in e-Health and imperatives for their adoption in Africa : research article.* 2013. **50**(1): p. 55-72.
47. Broyles, D., et al., *Chapter 7 - The Evolving Health Information Infrastructure*, in *Health Information Exchange*, B.E. Dixon, Editor. 2016, Academic Press. p. 107-122.
48. Alyea, J.M., et al., *Chapter 9 - Standardizing Health-Care Data Across an Enterprise*, in *Health Information Exchange*, B.E. Dixon, Editor. 2016, Academic Press. p. 137-148.
49. Lee, M., et al., *Developing a common health information exchange platform to implement a nationwide health information network in South Korea.* Healthc Inform Res, 2015. **21**(1): p. 21-29.
50. Appari, A. and M.E. Johnson, *Information Security and Privacy in Healthcare : Current State of Research.* International Journal of Internet Enterprise Management, 2010. **6**(4): p. 279-314.
51. World Health Organization. *Strengthening health security by implementing the International Health Regulations (2005)*. 2005 [cited 2020 20/05/2020]; Available from: https://www.who.int/ihr/about/en/.
52. International Telecommunication Union, *SDG Digital Investment Framework: A Whole-of-Government Approach to Investing in Digital Technologies to Achieve the SDGs*. 2019: Geneva, Swizerland. p. 136.
53. Stroetmann, K., *Digital Health Ecosystem for African Countries: A guide for Public and Private Actors for Establishing Holistic Digital Health Ecosystems in Africa*. 2018: Frankfurt, Germaney. p. 48.
54. Global Financing Facility and The World Bank, *Guidance Note: Investment Cases*. 2016: Washington DC. p. 17.
55. Measure Evaluation. *Global Digital Health Resources and Maturity Models: A Summary*. 2018 30/1/2021]; Available from: https://www.measureevaluation.org/resources/publications/fs-18-305#:~:text=Global%20Digital%20Health%20Resources%20and%20Maturity%20Models%3A%20A%20Summary,-Download%20Document%3A&text=Abstract%3A&text=A%20multidimensional%20maturity%20model%20focuses,of%20existing%20digital%20health%20capabilities.
56. Measure Evaluation. *Health Information Systems Interoperability Maturity Toolkit*. 2019 30/06/2021]; Available from: https://www.measureevaluation.org/tools/health-information-systems-interoperability-toolkit.html.
57. Simbini, T., et al., *Monitoring diseases across borders : African regional integrative information systems.* MEDINFO, 2010: p. 401-405.

Annexures

Annexure 1: Definitions

eHealth is the cost-effective and secure use of ICT in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research.

A Digital health ecosystem is the holistic application of information and communication technologies to support and improve healthcare delivery and its coordination and integration across providers in local, district, national and regional levels.

Data standards encompasses methods, protocols, terminologies, and specifications for the collection, exchange, storage, analysis and retrieval of information associated with healthcare applications, including medical records, medications, radiological images, payment and reimbursement, medical devices and monitoring systems, and administrative processes.

Digital health involves the development of interconnected health systems using computational technologies, smart devices, and communication media to aid healthcare professionals and patients in managing illnesses and health risks, as well as in promoting health and wellbeing.

Interoperability involves the ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged.

Privacy is the freedom to choose what information is shared or not shared with other parties.

Confidentiality is the obligation to keep secret information that one has been entrusted with.

Security is the combination of administrative, technical and physical safeguards that ensure confidentiality and promote privacy.

Health information exchange is defined as the electronic transfer of clinical and/or administration information among the organizations, people, and technology that hosts the defined ecosystems.

A standard is an agreed-upon, repeatable way of doing something.

Public health includes all the activities whose primary purpose is to promote, restore, and/or maintain the health across the continent, Member States or regions. This also refers to the people, institutions, resources, and policies that governments put in place to improve public health.

Universal health coverage means that all people and communities can use the promotive, preventive, curative, rehabilitative and palliative health services they need, of sufficient quality to be effective, while also ensuring that the use of these services does not expose the user to financial hardship.

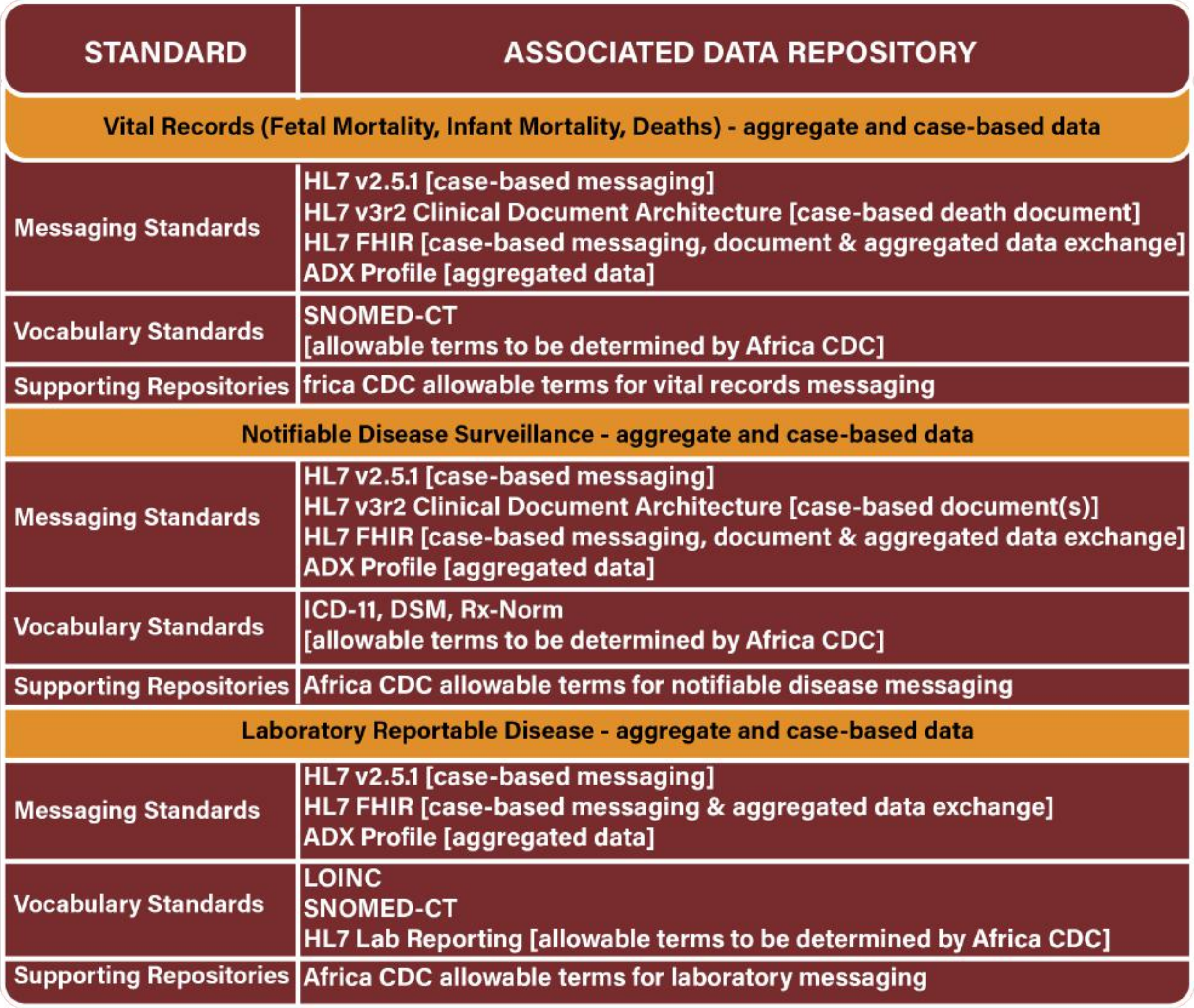
e-Surveillance is the use of digital devices to improve health data collection, sharing and outbreak detection across all levels of the health system.

Annexure 2: Reporting

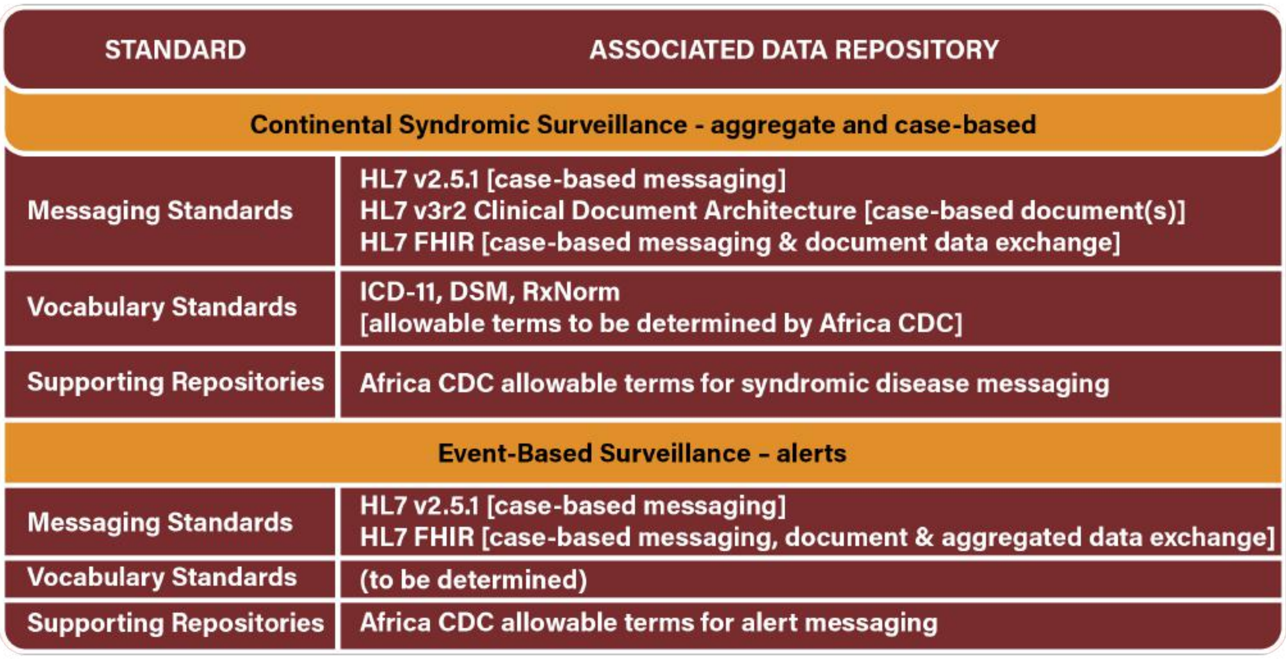
2.1. Reporting to Africa CDC from the Member States

This section addresses the messaging standards, vocabulary standards, and associated data repositories for each of these system boundaries. The Africa CDC recommends that AU Member States use the standards as described below for not only e-Surveillance data collection for the Africa CDC, but also for their internal e-Surveillance data collection between the National IDSR and reporting sub-national units, healthcare facilities and testing laboratories. Ideally, national, region/province and district level e-Surveillance will be a secure, seamless and interoperable implementation.

Table 7. Standards and Associated Repositories



STANDARD	ASSOCIATED DATA REPOSITORY
Vital Records (Fetal Mortality, Infant Mortality, Deaths) - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based death document] HL7 FHIR [case-based messaging, document & aggregated data exchange] ADX Profile [aggregated data]
Vocabulary Standards	SNOMED-CT [allowable terms to be determined by Africa CDC]
Supporting Repositories	frica CDC allowable terms for vital records messaging
Notifiable Disease Surveillance - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based document(s)] HL7 FHIR [case-based messaging, document & aggregated data exchange] ADX Profile [aggregated data]
Vocabulary Standards	ICD-11, DSM, Rx-Norm [allowable terms to be determined by Africa CDC]
Supporting Repositories	Africa CDC allowable terms for notifiable disease messaging
Laboratory Reportable Disease - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 FHIR [case-based messaging & aggregated data exchange] ADX Profile [aggregated data]
Vocabulary Standards	LOINC SNOMED-CT HL7 Lab Reporting [allowable terms to be determined by Africa CDC]
Supporting Repositories	Africa CDC allowable terms for laboratory messaging

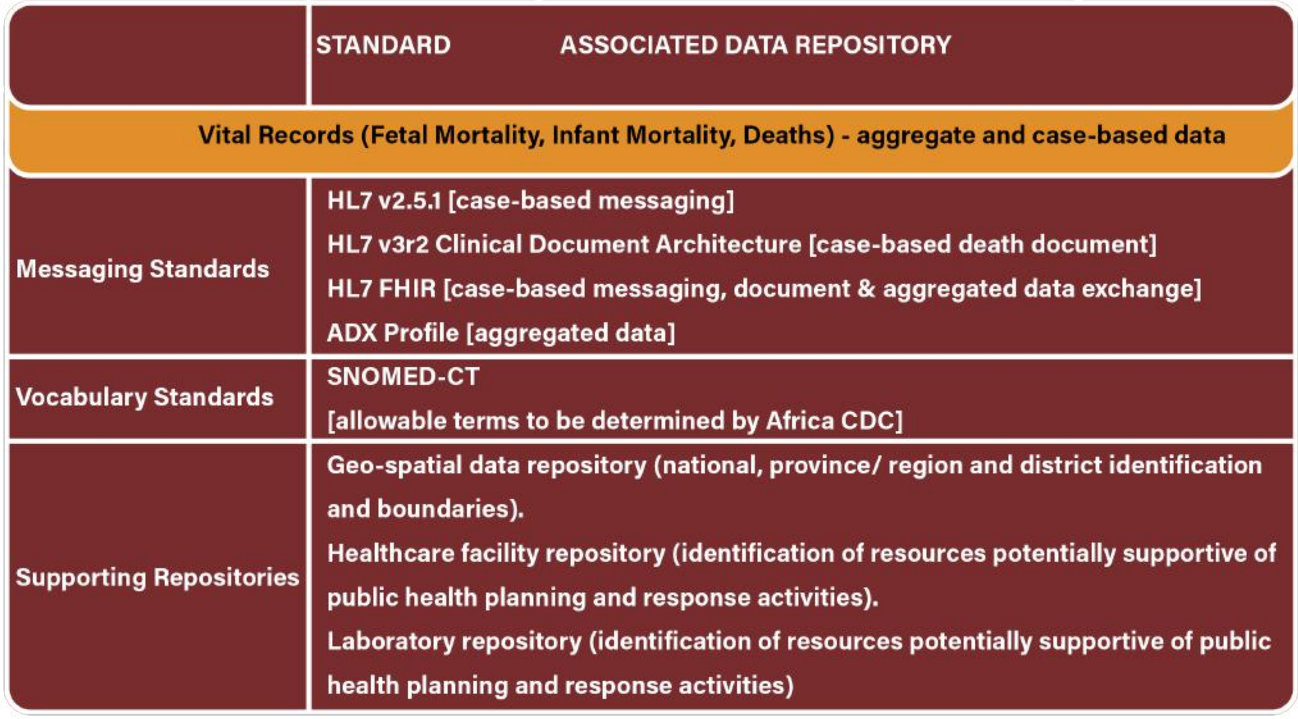


STANDARD	ASSOCIATED DATA REPOSITORY
Continental Syndromic Surveillance - aggregate and case-based	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based document(s)] HL7 FHIR [case-based messaging & document data exchange]
Vocabulary Standards	ICD-11, DSM, RxNorm [allowable terms to be determined by Africa CDC]
Supporting Repositories	Africa CDC allowable terms for syndromic disease messaging
Event-Based Surveillance - alerts	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 FHIR [case-based messaging, document & aggregated data exchange]
Vocabulary Standards	(to be determined)
Supporting Repositories	Africa CDC allowable terms for alert messaging

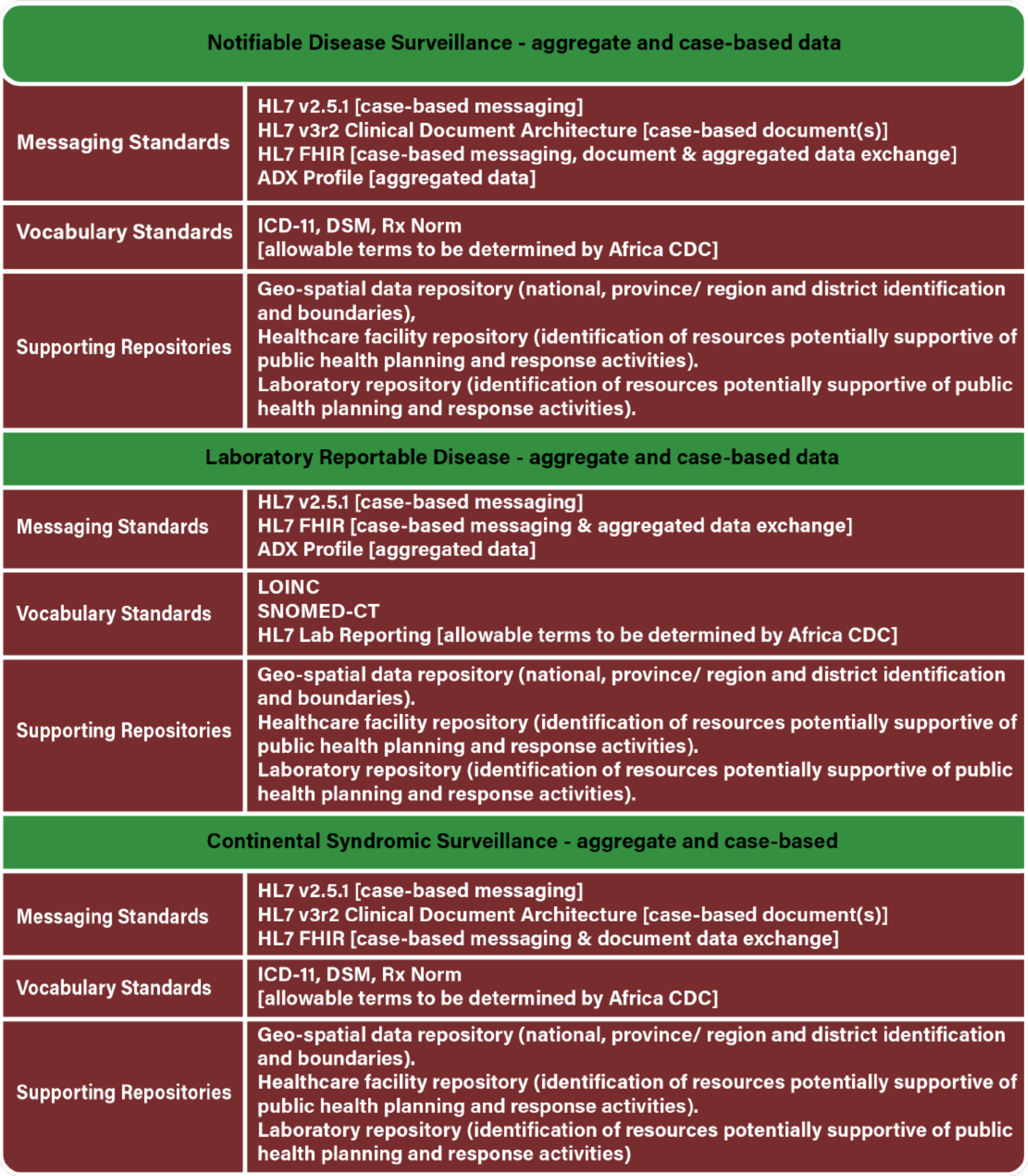
2.2. Reporting to National Authority (MOH, NPHI, or equivalent) from region/province

Africa CDC recommends that each Member State follow a similar model for messaging and vocabulary standards. Africa CDC recommends that identification of specific national e-Surveillance repositories be left to each Member State with the exception of the repositories recommended below.

Table 8. Standards and Associated Repositories – from Region/ Province to National



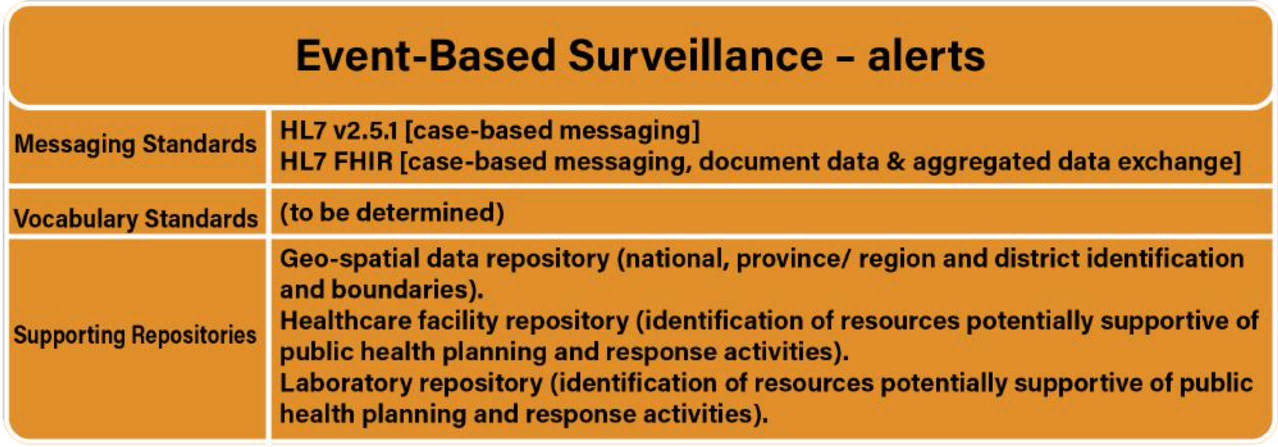
	STANDARD ASSOCIATED DATA REPOSITORY
Vital Records (Fetal Mortality, Infant Mortality, Deaths) - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based death document] HL7 FHIR [case-based messaging, document & aggregated data exchange] ADX Profile [aggregated data]
Vocabulary Standards	SNOMED-CT [allowable terms to be determined by Africa CDC]
Supporting Repositories	Geo-spatial data repository (national, province/ region and district identification and boundaries). Healthcare facility repository (identification of resources potentially supportive of public health planning and response activities). Laboratory repository (identification of resources potentially supportive of public health planning and response activities)



Notifiable Disease Surveillance - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based document(s)] HL7 FHIR [case-based messaging, document & aggregated data exchange] ADX Profile [aggregated data]
Vocabulary Standards	ICD-11, DSM, Rx Norm [allowable terms to be determined by Africa CDC]
Supporting Repositories	Geo-spatial data repository (national, province/ region and district identification and boundaries), Healthcare facility repository (identification of resources potentially supportive of public health planning and response activities). Laboratory repository (identification of resources potentially supportive of public health planning and response activities).

Laboratory Reportable Disease - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 FHIR [case-based messaging & aggregated data exchange] ADX Profile [aggregated data]
Vocabulary Standards	LOINC SNOMED-CT HL7 Lab Reporting [allowable terms to be determined by Africa CDC]
Supporting Repositories	Geo-spatial data repository (national, province/ region and district identification and boundaries). Healthcare facility repository (identification of resources potentially supportive of public health planning and response activities). Laboratory repository (identification of resources potentially supportive of public health planning and response activities).

Continental Syndromic Surveillance - aggregate and case-based	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based document(s)] HL7 FHIR [case-based messaging & document data exchange]
Vocabulary Standards	ICD-11, DSM, Rx Norm [allowable terms to be determined by Africa CDC]
Supporting Repositories	Geo-spatial data repository (national, province/ region and district identification and boundaries). Healthcare facility repository (identification of resources potentially supportive of public health planning and response activities). Laboratory repository (identification of resources potentially supportive of public health planning and response activities)



Event-Based Surveillance – alerts	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 FHIR [case-based messaging, document data & aggregated data exchange]
Vocabulary Standards	(to be determined)
Supporting Repositories	Geo-spatial data repository (national, province/ region and district identification and boundaries). Healthcare facility repository (identification of resources potentially supportive of public health planning and response activities). Laboratory repository (identification of resources potentially supportive of public health planning and response activities).

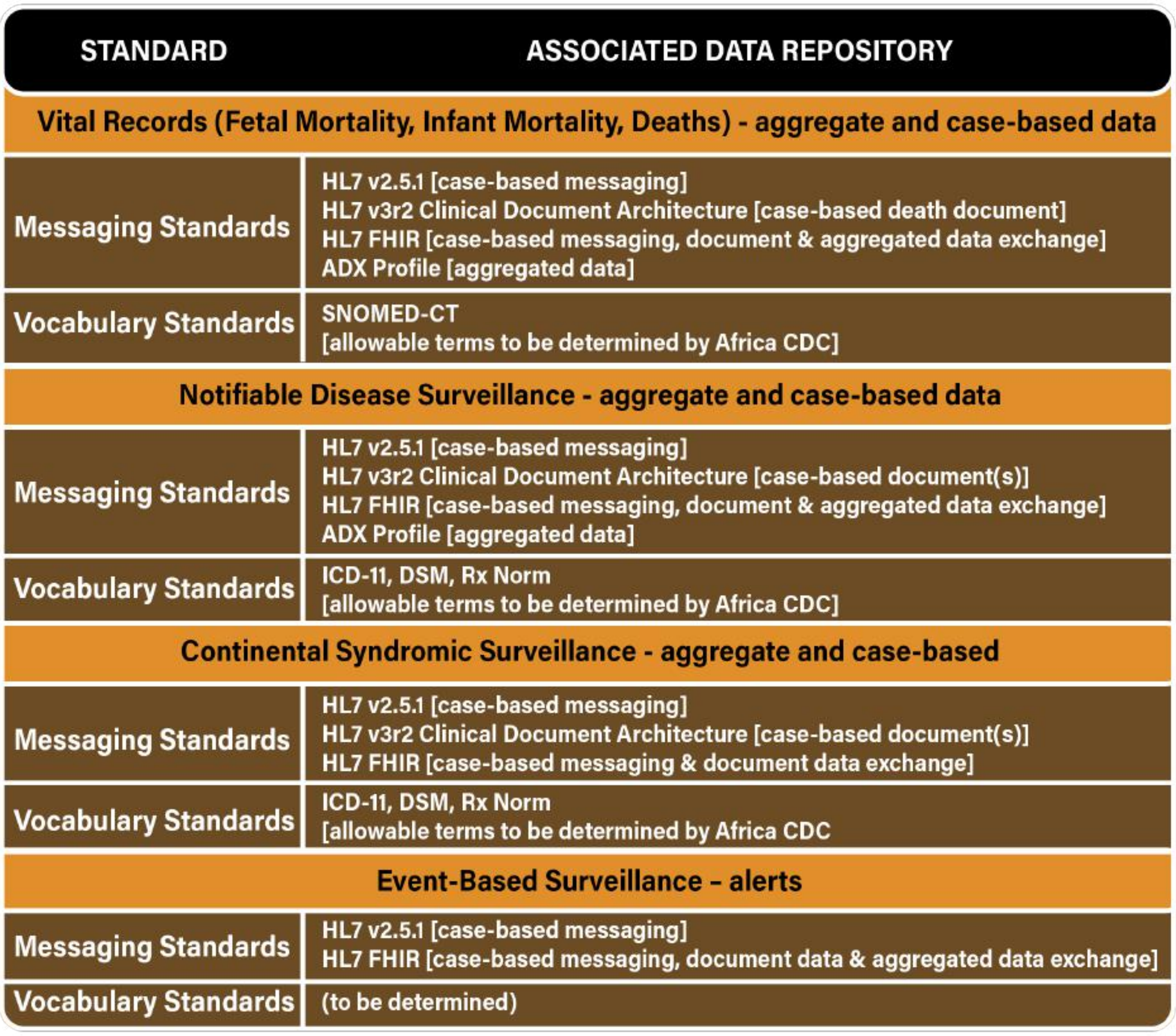
2.3. Reporting to region/province from district

Africa CDC recommends that each Member State follow a similar model for messaging and vocabulary standards between region/province and district as in Section 2.2 above. Additional repositories should be identified at the intermediate level as needed.

2.4. Reporting to district from health facility

Africa CDC recommends that each Member State follow a similar model for messaging and vocabulary standards between district and health facility as indicated below. Additional repositories should be identified at this lower level as needed. For purposes of reuse and cost effectiveness, it may be advantageous to AU Members to leverage a common platform for public health data reporting such that smaller clinics do not bear a disproportionate burden.

Table 9 Standards and Associated Repositories – from Health Facility to District

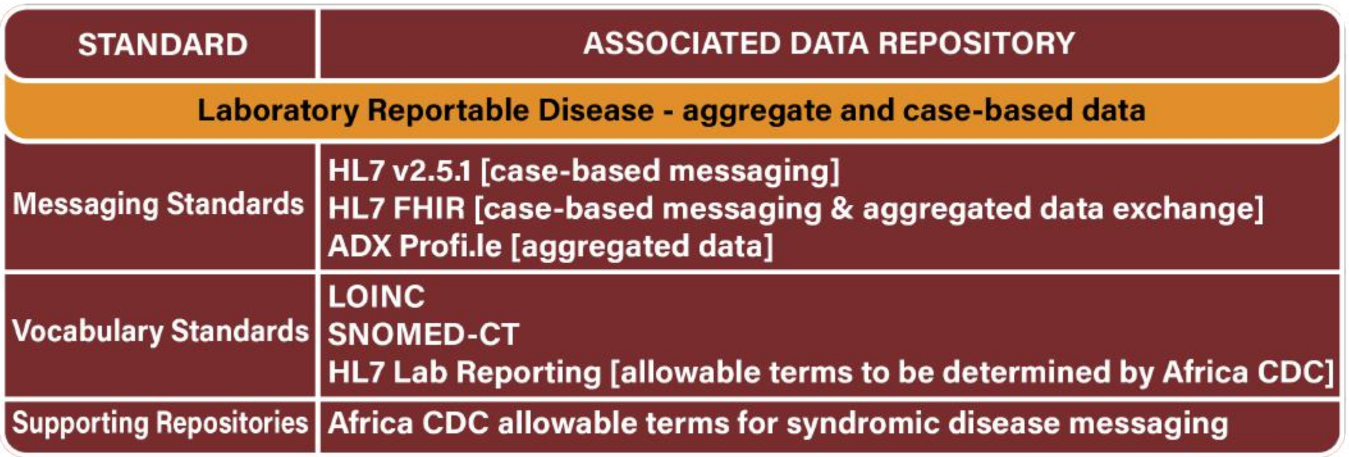


STANDARD	ASSOCIATED DATA REPOSITORY
Vital Records (Fetal Mortality, Infant Mortality, Deaths) - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based death document] HL7 FHIR [case-based messaging, document & aggregated data exchange] ADX Profile [aggregated data]
Vocabulary Standards	SNOMED-CT [allowable terms to be determined by Africa CDC]
Notifiable Disease Surveillance - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based document(s)] HL7 FHIR [case-based messaging, document & aggregated data exchange] ADX Profile [aggregated data]
Vocabulary Standards	ICD-11, DSM, Rx Norm [allowable terms to be determined by Africa CDC]
Continental Syndromic Surveillance - aggregate and case-based	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 v3r2 Clinical Document Architecture [case-based document(s)] HL7 FHIR [case-based messaging & document data exchange]
Vocabulary Standards	ICD-11, DSM, Rx Norm [allowable terms to be determined by Africa CDC
Event-Based Surveillance – alerts	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 FHIR [case-based messaging, document data & aggregated data exchange]
Vocabulary Standards	(to be determined)

2.5. Reporting from national LIMS

In the case where laboratory data is not integrated with the national e-Surveillance, Africa CDC recommends that each Member State follow the model below for messaging and vocabulary standards between Africa CDC e-Surveillance and a national LIMS.

Table 10. Standards and Associated Repositories – from National LIMS



STANDARD	ASSOCIATED DATA REPOSITORY
Laboratory Reportable Disease - aggregate and case-based data	
Messaging Standards	HL7 v2.5.1 [case-based messaging] HL7 FHIR [case-based messaging & aggregated data exchange] ADX Profi.le [aggregated data]
Vocabulary Standards	LOINC SNOMED-CT HL7 Lab Reporting [allowable terms to be determined by Africa CDC]
Supporting Repositories	Africa CDC allowable terms for syndromic disease messaging

2.6. Reporting from Regional Laboratory Information System (LIS)

In the case where laboratory data is not integrated with the national e-Surveillance or LIMS, Africa CDC recommends that each Member State follow the model in Section 2.5 above for messaging and vocabulary standards between Africa CDC e-Surveillance and a regional LIS. As needed, additional repositories should be identified at this lower level. It may be advantageous for AU Members to leverage a common platform for public health data reporting for reuse and cost-effectiveness purposes, so that smaller laboratories are not burdened disproportionately.

Annexure 3: HIE Development Principles and Best Practice

HIE development principles (as described at https://digitalprinciples.org)

- ***Design with the user*** - partner with AU Member organizations throughout the development and implementation lifecycle, co-create solutions, and continuously gather and incorporate users' feedback.
- ***Understand the existing ecosystem*** - consider the particular structures and needs that exist in each AU Member state, region and community.
- ***Design for scale and continental adoption*** - think beyond any initial Africa CDC pilot implementations with individual AU Members and instead make choices to enable widespread adoption by all AU Members, and determine what will be affordable and usable by a Member or region rather than by a few pilot AU states with the long-term objective of continental information exchange [57]. Moreover, a coordinated Africa CDC-led programme of testing and development of different aspects of guidelines and policy so that appropriate country "use cases" can be developed, within an "action learning" framework that is intended to find solutions to the pressing problems that may hamper intra and inter-country information exchange.
- ***Build for sustainability*** - build sustainable programs, platforms and digital tools to maintain user and stakeholder support, and to maximize long-term impact.
- ***Be data driven*** - ensure quality information is available to the right people when they need it, and that they are using those data to take appropriate actions and responses for reportable diseases.
- ***Use open standards, open source, open data and open innovation*** - increase collaboration with the AU (and other) digital development communities to avoid duplicating work.
- ***Reuse and improve*** - look for ways to adapt and enhance existing tools, resources and approaches.
- ***Address privacy and security*** - carefully consider which data are collected and how these data are acquired, used, stored and shared.
- ***Be collaborative*** - share information, insights, strategies and resources with AU Members to achieve increased e-Surveillance efficiency and impact.

Support platform best practices

- The e-Surveillance platform(s) should be housed in secure facilities with controlled access for only authorized personnel.
- The e-Surveillance platform should be protected from unauthorized access and provide role-based access to the data for security and protection.
- A secure, remote recovery/backup site should be available in the event of damage to, or loss of, the primary e-Surveillance platform and/or facility.
- E-Surveillance system and data back-ups should be stored at a secure, remote storage site.
- E-Surveillance support facilities should use sustainable power sources and provide backup power sources and power generation capability in the event of power loss and/or outages.
- E-Surveillance system should support at least 99.9% availability (i.e., total downtime per year should be no more than 526 minutes). In the event of an unplanned downtime event for the e-Surveillance system, recovery to the remote site should occur within a 2-hour timeframe.
- Where possible, the e-Surveillance system should link with multiple internet service providers (e.g., at least two separate providers) for operations continuity in the event of an Internet Services Provider outage.
- E-Surveillance system should employ a hardware and/or software firewall.
- E-Surveillance should use proven free and open software where feasible, and collaborate with open software organizations to extend existing products to meet e-Surveillance needs.
- E-Surveillance team should test and verify all software and system updates on a separate (but potentially scaled down) staging system prior to deployment and use.

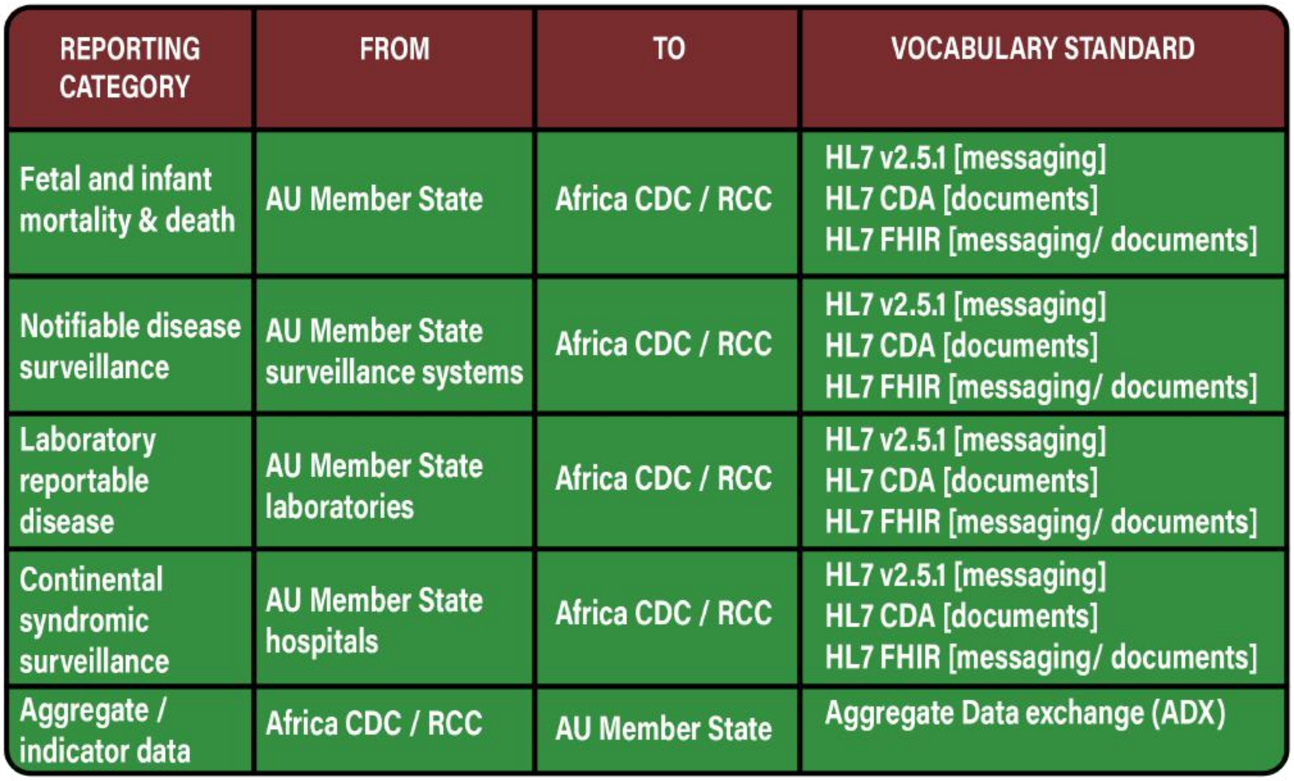
Message processing minimum functions

- Assign unique anonymous identifier to case-based records traversing the system; this will prevent the potential collision of AU Member State unique case identifiers.
- Extract PII as needed when sharing and re-transmitting data from one AU State to another.
- Reformat messages into the appropriate recipient-required format (e.g., e-mail, secure file, or web page message).
- Enforce the quality of message structure and content.

Annexure 4: Mapping Messaging Standards to Africa CDC Reporting Categories

The table below maps the messaging standards to different Africa CDC reporting categories. Note that actual message content and fields will be separately determined by the Africa CDC in coordination with AU Member States.

Table 11. Mapping Messaging Standards

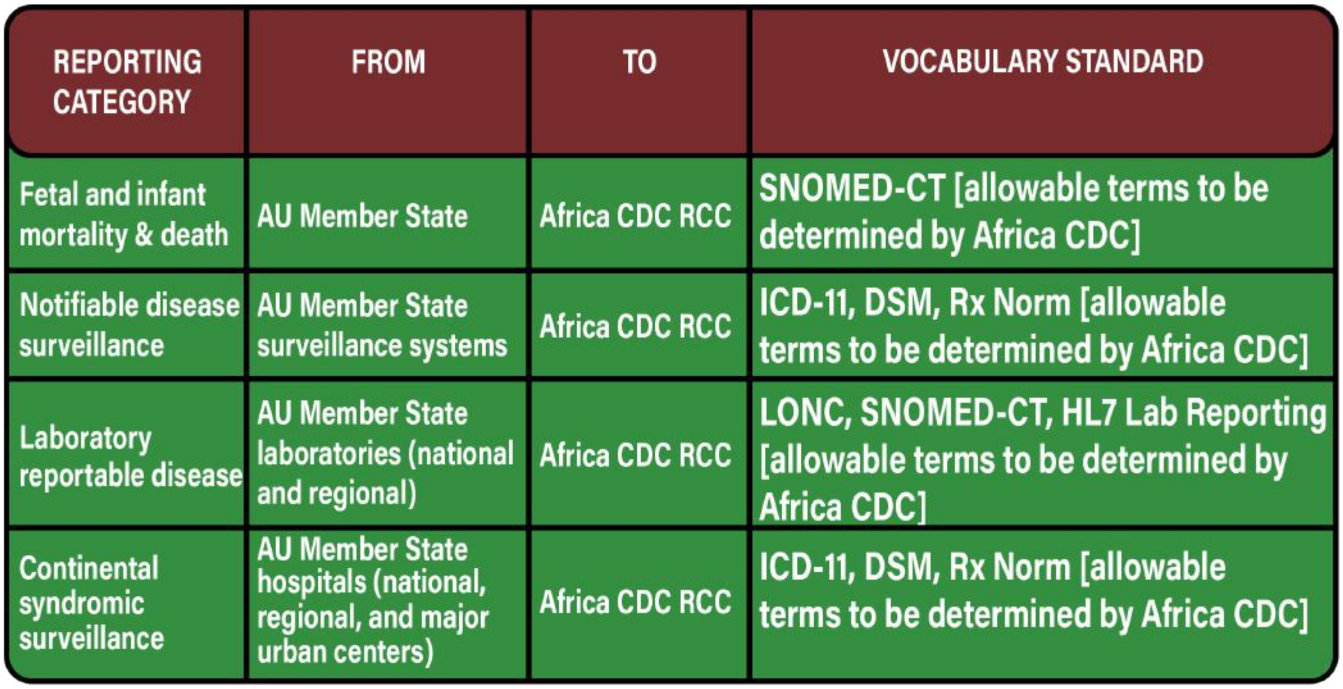


REPORTING CATEGORY	FROM	TO	VOCABULARY STANDARD
Fetal and infant mortality & death	AU Member State	Africa CDC / RCC	HL7 v2.5.1 [messaging] HL7 CDA [documents] HL7 FHIR [messaging/ documents]
Notifiable disease surveillance	AU Member State surveillance systems	Africa CDC / RCC	HL7 v2.5.1 [messaging] HL7 CDA [documents] HL7 FHIR [messaging/ documents]
Laboratory reportable disease	AU Member State laboratories	Africa CDC / RCC	HL7 v2.5.1 [messaging] HL7 CDA [documents] HL7 FHIR [messaging/ documents]
Continental syndromic surveillance	AU Member State hospitals	Africa CDC / RCC	HL7 v2.5.1 [messaging] HL7 CDA [documents] HL7 FHIR [messaging/ documents]
Aggregate / indicator data	Africa CDC / RCC	AU Member State	Aggregate Data exchange (ADX)

Annexure 5: Mapping Vocabulary Standards to Africa CDC Reporting Categories

The table below maps the vocabulary standards to different Africa CDC reporting categories. Note that the subset of allowable terms and codes from vocabulary standards will be separately determined by the Africa CDC in coordination with AU Member States.

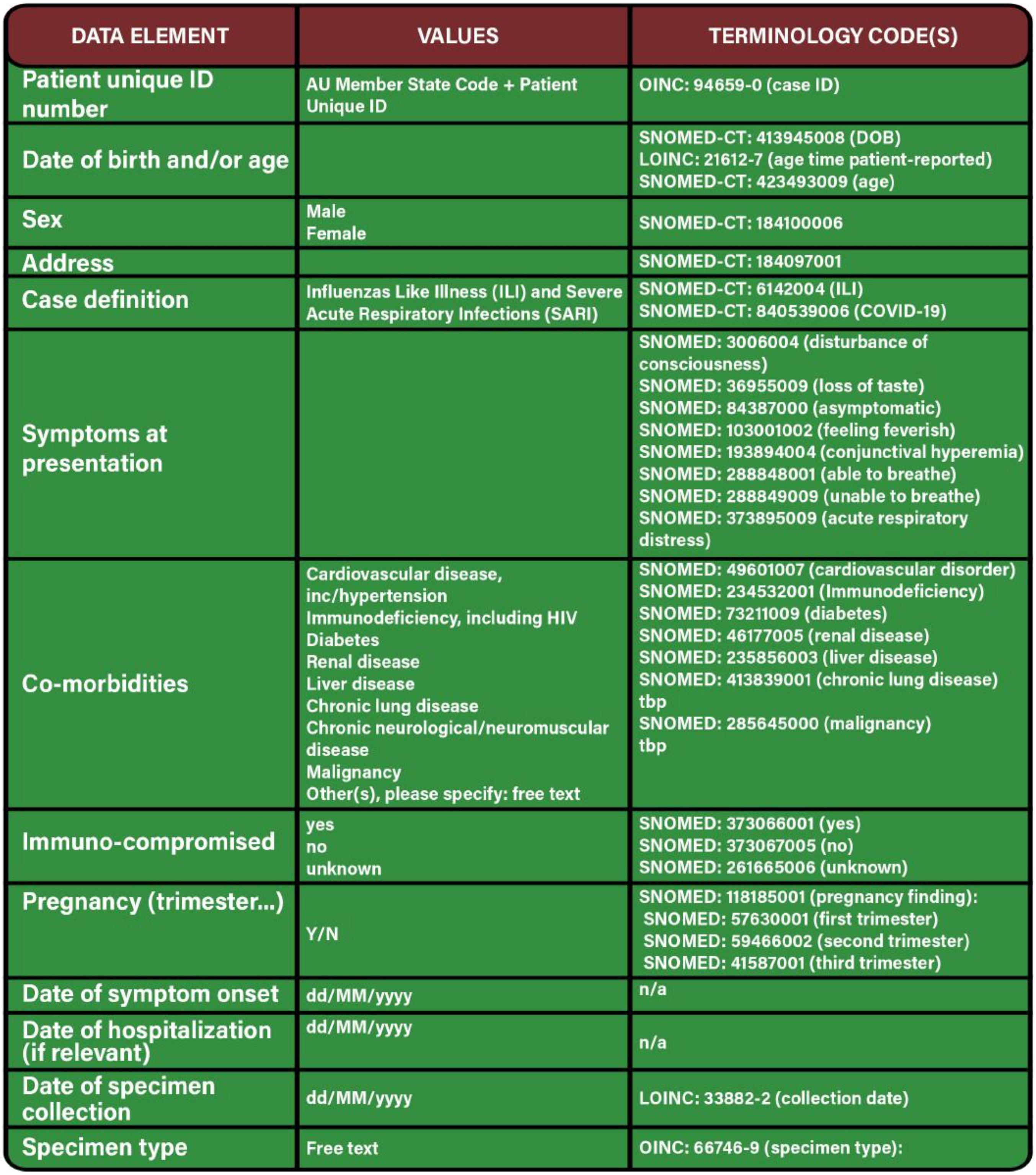
Table 12. Mapping Vocabulary Standards



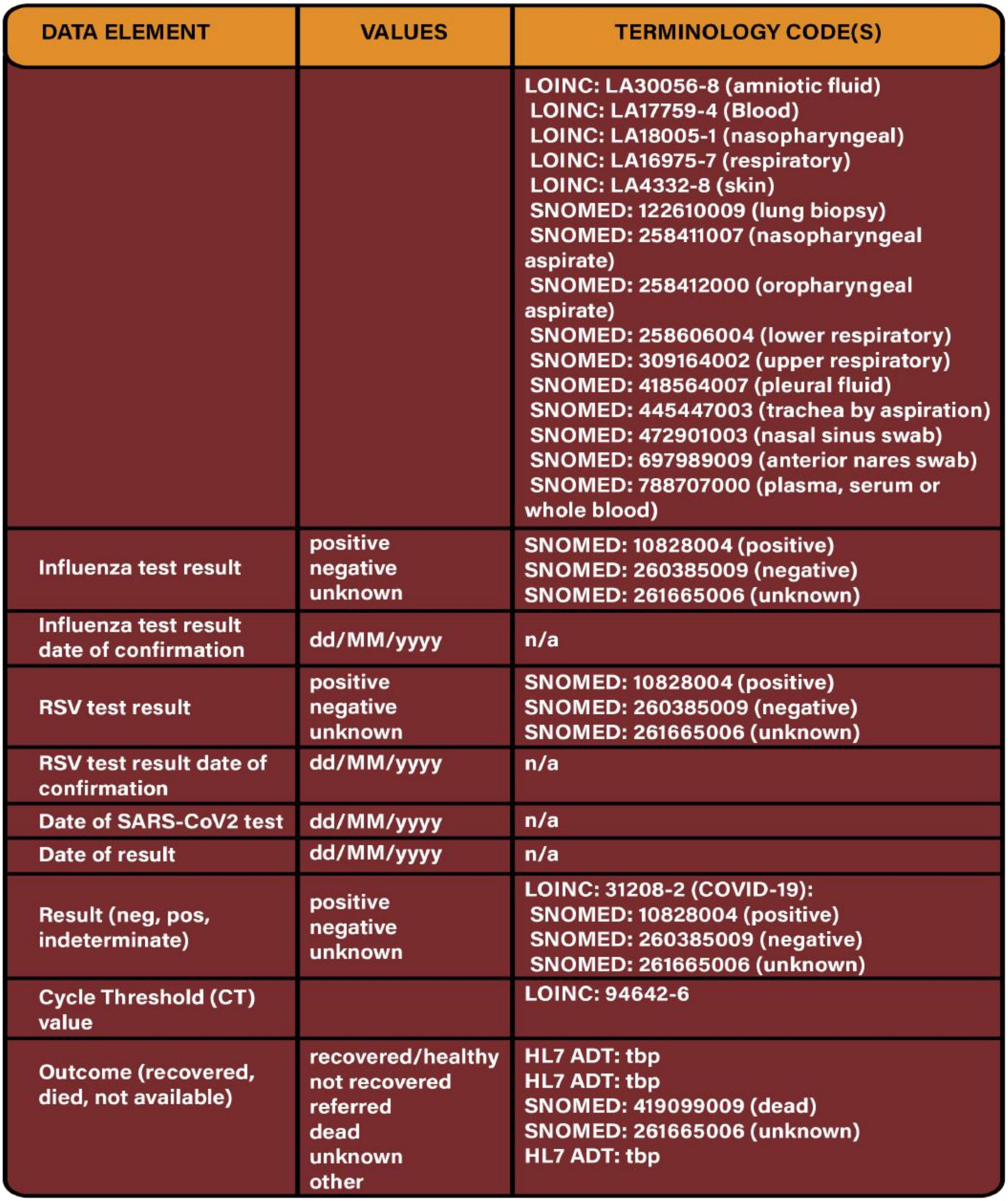
REPORTING CATEGORY	FROM	TO	VOCABULARY STANDARD
Fetal and infant mortality & death	AU Member State	Africa CDC RCC	SNOMED-CT [allowable terms to be determined by Africa CDC]
Notifiable disease surveillance	AU Member State surveillance systems	Africa CDC RCC	ICD-11, DSM, Rx Norm [allowable terms to be determined by Africa CDC]
Laboratory reportable disease	AU Member State laboratories (national and regional)	Africa CDC RCC	LONC, SNOMED-CT, HL7 Lab Reporting [allowable terms to be determined by Africa CDC]
Continental syndromic surveillance	AU Member State hospitals (national, regional, and major urban centers)	Africa CDC RCC	ICD-11, DSM, Rx Norm [allowable terms to be determined by Africa CDC]

Annexure 6: COVID-19 Minimal Surveillance and Reporting Transaction Set by Reporting Category

Table 13. COVID-19 Minimal Surveillance and Reporting Transactions by Category



DATA ELEMENT	VALUES	TERMINOLOGY CODE(S)
Patient unique ID number	AU Member State Code + Patient Unique ID	OINC: 94659-0 (case ID)
Date of birth and/or age		SNOMED-CT: 413945008 (DOB) LOINC: 21612-7 (age time patient-reported) SNOMED-CT: 423493009 (age)
Sex	Male Female	SNOMED-CT: 184100006
Address		SNOMED-CT: 184097001
Case definition	Influenzas Like Illness (ILI) and Severe Acute Respiratory Infections (SARI)	SNOMED-CT: 6142004 (ILI) SNOMED-CT: 840539006 (COVID-19)
Symptoms at presentation		SNOMED: 3006004 (disturbance of consciousness) SNOMED: 36955009 (loss of taste) SNOMED: 84387000 (asymptomatic) SNOMED: 103001002 (feeling feverish) SNOMED: 193894004 (conjunctival hyperemia) SNOMED: 288848001 (able to breathe) SNOMED: 288849009 (unable to breathe) SNOMED: 373895009 (acute respiratory distress)
Co-morbidities	Cardiovascular disease, inc/hypertension Immunodeficiency, including HIV Diabetes Renal disease Liver disease Chronic lung disease Chronic neurological/neuromuscular disease Malignancy Other(s), please specify: free text	SNOMED: 49601007 (cardiovascular disorder) SNOMED: 234532001 (Immunodeficiency) SNOMED: 73211009 (diabetes) SNOMED: 46177005 (renal disease) SNOMED: 235856003 (liver disease) SNOMED: 413839001 (chronic lung disease) tbp SNOMED: 285645000 (malignancy) tbp
Immuno-compromised	yes no unknown	SNOMED: 373066001 (yes) SNOMED: 373067005 (no) SNOMED: 261665006 (unknown)
Pregnancy (trimester...)	Y/N	SNOMED: 118185001 (pregnancy finding): SNOMED: 57630001 (first trimester) SNOMED: 59466002 (second trimester) SNOMED: 41587001 (third trimester)
Date of symptom onset	dd/MM/yyyy	n/a
Date of hospitalization (if relevant)	dd/MM/yyyy	n/a
Date of specimen collection	dd/MM/yyyy	LOINC: 33882-2 (collection date)
Specimen type	Free text	OINC: 66746-9 (specimen type):



DATA ELEMENT	VALUES	TERMINOLOGY CODE(S)
		LOINC: LA30056-8 (amniotic fluid) LOINC: LA17759-4 (Blood) LOINC: LA18005-1 (nasopharyngeal) LOINC: LA16975-7 (respiratory) LOINC: LA4332-8 (skin) SNOMED: 122610009 (lung biopsy) SNOMED: 258411007 (nasopharyngeal aspirate) SNOMED: 258412000 (oropharyngeal aspirate) SNOMED: 258606004 (lower respiratory) SNOMED: 309164002 (upper respiratory) SNOMED: 418564007 (pleural fluid) SNOMED: 445447003 (trachea by aspiration) SNOMED: 472901003 (nasal sinus swab) SNOMED: 697989009 (anterior nares swab) SNOMED: 788707000 (plasma, serum or whole blood)
Influenza test result	positive negative unknown	SNOMED: 10828004 (positive) SNOMED: 260385009 (negative) SNOMED: 261665006 (unknown)
Influenza test result date of confirmation	dd/MM/yyyy	n/a
RSV test result	positive negative unknown	SNOMED: 10828004 (positive) SNOMED: 260385009 (negative) SNOMED: 261665006 (unknown)
RSV test result date of confirmation	dd/MM/yyyy	n/a
Date of SARS-CoV2 test	dd/MM/yyyy	n/a
Date of result	dd/MM/yyyy	n/a
Result (neg, pos, indeterminate)	positive negative unknown	LOINC: 31208-2 (COVID-19): SNOMED: 10828004 (positive) SNOMED: 260385009 (negative) SNOMED: 261665006 (unknown)
Cycle Threshold (CT) value		LOINC: 94642-6
Outcome (recovered, died, not available)	recovered/healthy not recovered referred dead unknown other	HL7 ADT: tbp HL7 ADT: tbp SNOMED: 419099009 (dead) SNOMED: 261665006 (unknown) HL7 ADT: tbp

Annexure 7: Common Data Elements for COVID-19 Aggregated Data Reporting

At the continental level, the following data on COVID-19 cases are important for surveillance and coordinating pandemic response efforts:

- Number of laboratory-confirmed cases of COVID-19
  - Confirmed cases can be given the ICD-10 code U07.1 (Source- https://www.who.int/classifications/icd/covid19/en/)
  - Confirmed cases can be given the ICD-11 code RA01.0
- Number of COVID-19 laboratory tests with results
  - This allows calculation of positivity
- Number of persons under investigation (PUI) for COVID-19
  - Non-confirmed cases, or cases where laboratory testing is not available, can be given the ICD-10 code U07.2 (https://www.who.int/classifications/icd/covid19/en/)
  - Non-confirmed cases, or cases where laboratory testing is not available, can be given the ICD-11 code RA01.1
- Number of deaths caused by COVID-19
  - Both ICD-10 codes, U07.1 and U07.2, may be used for mortality coding as a cause of death
- Number of individuals, lab confirmed or PUIs, who are in the hospital with COVID
- Number of individuals, lab confirmed or PUIs, who are in an ICU
- Number of individuals (non-COVID) who are in a critical care unit
- Number of critical care beds available for new patients, COVID or non-COVID
- Number of individuals, lab confirmed or PUIs, who are currently on a ventilator
- Number of individuals (non-COVID) who are currently on a ventilator
- Number of ventilators available for new patients (COVID or non-COVID)
- Percentage of health care workers (HCWs) infected or quarantined at home

Data on COVID-19 cases are critical to report within 24 hours given the need to quickly identify cases and monitor progress towards ‘bending the curve’ of a pandemic illness. Contact tracing and the management of resources within a country will be performed by the Ministry of Health in each country. Africa CDC needs to track the disease at the continental level and support nations with their local efforts in consultation with Ministries.

Annexure 8: Common Data Elements for HIV Aggregated Data Reporting

At the continental level, the following data on HIV cases are important for surveillance and coordinating HIV response efforts:

(source: https://www.who.int/hiv/data/UA2011_indicator_guide_en.pdf)

- Testing and counselling
  - Number of health facilities that provide HIV testing and counselling services
  - Number of women and men aged 15 and older who received HIV Testing and Counselling (T&C) in the last 12 months and know their results
  - Percentage of women and men aged 15-49 who received an HIV test in the last 12 months and who know their results
  - Percentage of most-at-risk populations who received an HIV test in the last 12 months and who know their results
  - Number of recency tests administered
  - Percentage of positive recent infections
- Prevention in health care settings
  - Percentage of health care facilities where all therapeutic injections are given with new, disposable, single-use injection equipment
  - Number of health facilities with post-exposure prophylaxis services available on site
- Prevention of sexual transmission of HIV and prevention of transmission through injecting drug use
  - Estimated number of injecting drug users (IDUs)
  - Number of needle and syringe program (NSP) sites
  - Number of people on opioid substitution therapy
  - Number of syringes/needles distributed by NSP
  - Percentage of IDUs reporting the use of sterile injecting equipment the last time they injected

  - Percentage of IDUs reporting the use of a condom the last time they had sexual intercourse
  - Percentage of female and male sex workers (SWs) reporting the use of a condom with their most recent client
  - Percentage of men reporting the use of a condom the last time they had anal sex with a male partner
  - Percentage of most-at-risk populations (IDUs-C6a, SWs-C6b, MSM-C6c) who are HIV- infected
- Care
  - Percentage of adults and children enrolled in HIV care and eligible for co-trimoxazole (CTX) prophylaxis (according to national guidelines) currently receiving CTX prophylaxis
- HIV/TB
  - Number of health-care facilities providing ART services for people living with HIV with demonstrable infection control practices that include TB control
  - Percentage of estimated HIV-positive incident TB cases that received treatment for TB and HIV
  - Percentage of adults and children newly enrolled in HIV care starting isoniazid preventive therapy (IPT)
  - Percentage of adults and children enrolled in HIV care who had TB status assessed and recorded during their last visit
- Sexually transmitted infections
  - Percentage of women accessing antenatal care (ANC) services who were tested for syphilis at first ANC visit
  - Percentage of ANC attendees who were positive for syphilis
  - Percentage of ANC attendees positive for syphilis who received treatment
  - Percentage of SWs with active syphilis
  - Percentage of men who have sex with men with active syphilis

- Antiretroviral therapy
    - Number of health facilities that offer ART
    - Percentage of eligible adults and children currently receiving ART
    - Number of eligible adults and children who newly initiated ART during the reporting period (2010)
    - Percentage of adults and children with HIV still alive and known to be on ART:
        - 12 months after initiating treatment among patients starting ART during 2009
        - 24 months after initiating treatment among patients initiating ART during 2008
        - 60 months after initiating treatment among patients initiating ART during 2005
- Health systems
    - Percentage of health facilities dispensing ARVs that experienced a stock-out of at least one required ARV in the last 12 months
    - Percentage of facilities providing ART using CD4 monitoring in line with national guidelines/policies, on-site or through referral
- Women and children
    - Number of pregnant women attending ANC at least once during the reporting
    - Number of health facilities providing ANC services
    - Number of health facilities providing ANC services that also provide HIV testing and counselling for pregnant women
    - Number of health facilities providing ANC services that offer both HIV testing and antiretrovirals for the prevention of mother-to-child transmission on-site
    - Number of health facilities providing ANC services which also provide CD4 testing on-site, or have a system for collecting and transporting blood samples for CD4 testing for HIV-infected pregnant women

- Number of health facilities that offer pediatric ART
- Percentage of health facilities that provide virological testing services (e.g. PCR) for diagnosis of HIV in infants on-site or from dried blood spots (DBS)
- Percentage of pregnant women who were tested for HIV and received their results - during pregnancy, during labor and delivery, and during the post-partum period (<72 hours), including those with previously known HIV status
- Percentage of pregnant women attending ANC whose male partner was tested for HIV
- Percentage of HIV-infected pregnant women assessed for ART eligibility through either clinical staging or CD4 testing 69 #I8a
- Percentage of HIV-infected pregnant women who received antiretroviral drugs to reduce the risk of mother-to-child transmission (MTCT)
- Percentage of infants born to HIV-infected women receiving ARV for prophylaxis for the prevention of mother-to-child transmission (PMTCT)
- Percentage of infants born to HIV-infected women started on CTX prophylaxis within two months of birth
- Percentage of infants born to HIV-infected women receiving a virological test for HIV within 2 months of birth
- Distribution of feeding practices (exclusive breastfeeding, replacement feeding, mixed feeding/other) for infants born to HIV-infected women at DPT3 visit
- Percentage of HIV-infected children aged 0–14 years who are currently receiving ART

Data on HIV cases should be reported to Africa CDC on a monthly basis.

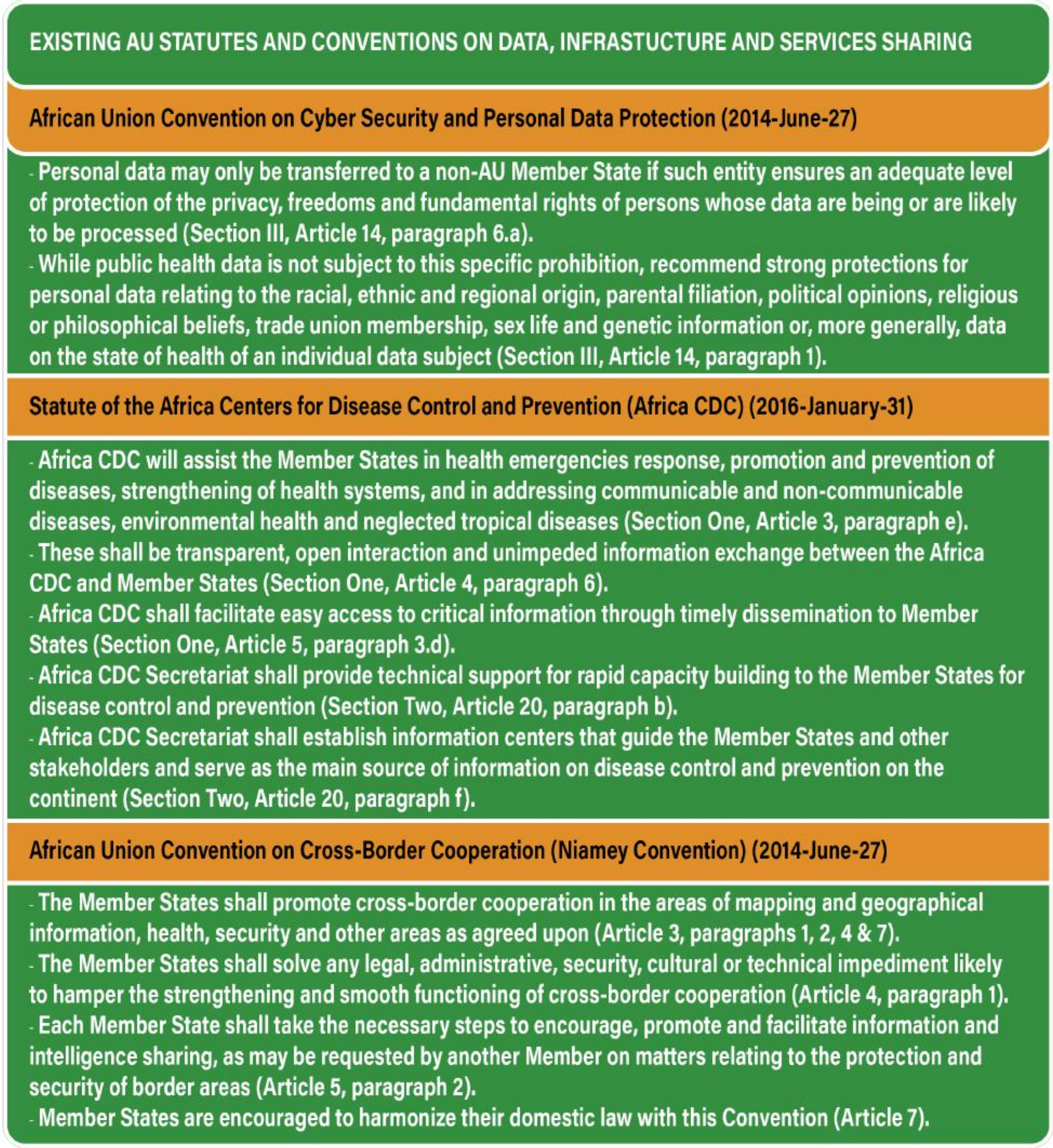
Annexure 9: Prerequisites of Successful Implementation of Cloud-based Infrastructure and Services

a) ***Understanding the global impact of cloud computing*** - It is possible to own and control HIE for e-surveillance data, services, and tools using the cloud computing model while leveraging existing infrastructure and services from one or more third-party providers. Zambia has integrated data from multiple sources (e.g., Smart Health EMR, DHIS2, etc.) into a cloud environment over the last three years to improve data quality, visibility, and responsiveness. To great success, the US CDC has adopted a cloud model for its internal email, voice over IP, and business productivity applications (Microsoft Office 365). (especially in the light of disruptions due to the COVID-19 pandemic). It also employs a cloud model to enable the rapid deployment of public health applications to individual states and jurisdictions. The UK Cloud is used by the United Kingdom (UK) for its National Health Services (NHS).

b) ***Legal framework for cloud computing*** - Moving data to the cloud necessitates a legal framework to adequately protect national data stored in the cloud while also ensuring individual data privacy for public health purposes. The African Union Convention On Cyber Security And Personal Data Protection (2014-June-27) requires open sharing of public health data among Africa CDC and Member States, and when combined with the data sharing agreement established in Section A of this document, provides protections and controls for both national data stored in the cloud as well as individual data privacy, while allowing appropriate use of these data for continental public health purposes. In the European Union (EU), EU Directive 95/46/EC of 1995 requires the protection of natural persons' fundamental rights and freedoms, particularly their right to privacy in relation to the processing of personal data. The recent U.S. CLOUD (Clarifying Lawful Overseas Use of Data Act) Act of 2018 allows U.S. law enforcement to compel U.S.-based technology companies to provide requested data stored on servers whether the data is stored in the US or in a foreign country via lawful warrant or subpoena; the act includes mechanisms for companies or courts to reject or challenge a warrant or subpoena if it is believed that the request violates the privacy Entity-based Africa CDC data related to U.S. citizens (e.g., U.S. patients treated by an African healthcare provider for a reportable disease) may be subject to CLOUD Act requests and the requirement that data on any U.S. citizen be appropriately protected (as is the case here based on Section B policies and Section C privacy and security standards); however, this should have no impact on the privacy rights of AU citizens.

c) ***Cross-border standardization and regulation*** - The HIE for e-Surveillance concept architecture envisions cross-border sharing of public health data at the continental level, as well as the use of that data to support rapid response to diseases that may affect multiple Member States. Existing AU statutes and conventions establish the foundation for cross-border data, infrastructure, and service sharing, specifically:

d) **Table 14. Existing AU Statutes and Conventions on Data, Infrastructure and Service Sharing**



EXISTING AU STATUTES AND CONVENTIONS ON DATA, INFRASTUCTURE AND SERVICES SHARING
African Union Convention on Cyber Security and Personal Data Protection (2014-June-27)
- Personal data may only be transferred to a non-AU Member State if such entity ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed (Section III, Article 14, paragraph 6.a). - While public health data is not subject to this specific prohibition, recommend strong protections for personal data relating to the racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of an individual data subject (Section III, Article 14, paragraph 1).
Statute of the Africa Centers for Disease Control and Prevention (Africa CDC) (2016-January-31)
- Africa CDC will assist the Member States in health emergencies response, promotion and prevention of diseases, strengthening of health systems, and in addressing communicable and non-communicable diseases, environmental health and neglected tropical diseases (Section One, Article 3, paragraph e). - These shall be transparent, open interaction and unimpeded information exchange between the Africa CDC and Member States (Section One, Article 4, paragraph 6). - Africa CDC shall facilitate easy access to critical information through timely dissemination to Member States (Section One, Article 5, paragraph 3.d). - Africa CDC Secretariat shall provide technical support for rapid capacity building to the Member States for disease control and prevention (Section Two, Article 20, paragraph b). - Africa CDC Secretariat shall establish information centers that guide the Member States and other stakeholders and serve as the main source of information on disease control and prevention on the continent (Section Two, Article 20, paragraph f).
African Union Convention on Cross-Border Cooperation (Niamey Convention) (2014-June-27)
- The Member States shall promote cross-border cooperation in the areas of mapping and geographical information, health, security and other areas as agreed upon (Article 3, paragraphs 1, 2, 4 & 7). - The Member States shall solve any legal, administrative, security, cultural or technical impediment likely to hamper the strengthening and smooth functioning of cross-border cooperation (Article 4, paragraph 1). - Each Member State shall take the necessary steps to encourage, promote and facilitate information and intelligence sharing, as may be requested by another Member on matters relating to the protection and security of border areas (Article 5, paragraph 2). - Member States are encouraged to harmonize their domestic law with this Convention (Article 7).

e) ***Data centers*** - As mentioned in Section 9.1, multiple cloud infrastructure providers are expanding their presence in Africa by establishing data centers on the continent. The largest providers, in particular, Amazon, Google, and Microsoft, are investing on the African continent to support cloud computing and cloud-based shared services, which are required for Africa CDC HIE for e-Surveillance. Africa CDC recommends soliciting information from such cloud service providers to determine whether they can meet the needs of the HIE for e-Surveillance platform, and if so, soliciting formal bids for services from those deemed most qualified (i.e., a Tier 3 or Tier 4 data center guaranteeing at least 99.9% availability with externally audited operations per SAS 70 (Statement on Auditing Standards No. 70), SAEC 16 (Statements on Standards for Auditing and Assessment.

f) ***Trust in providers*** - The HIE for e-Surveillance necessitates a well-defined, transparent, and ongoing audit of provider (best practice) processes to ensure ongoing compliance with minimum defined cloud-based data center standards; the provider's security model and processes; the provider's backup and recovery model and processes; the provider's platform accessibility and ease of transfer of Africa CDC data and tools in the event of provider failure (e.g., primary provider for service with an alt provider).

Annexure 10: COVID-19 Case-Based Surveillance References

- Africa Centers for Disease Control and Prevention (Africa CDC), Protocol for Enhanced Severe Acute Respiratory Illness and Influenza-Like Illness Surveillance for COVID-19 in Africa, March 2020; [https://africacdc.org/download/protocol-for-enhanced-severe-acute-respiratory-illness-and-influenza-like-illness-surveillance-for-covid-19-in-africa/] identifies COVID-19 case definitions, minimum data sets for reporting.

- Africa Centers for Disease Control and Prevention (Africa CDC), COVID-19 [https://africacdc.org/covid-19/]; provides dashboard, policy documents, and other resources related to COVID-19.

- World Health Organization (WHO), Coronavirus disease (COVID-19) technical guidance: Surveillance and case definitions, [https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/surveillance-and-case-definitions]; provides recommended case-based reporting form, case-based reporting data dictionary and Aggregated Weekly Reporting Form.

- Association of Public Health Laboratories (APHL), Responding to the Coronavirus Disease (COVID-19) Pandemic [https://www.aphl.org/programs/preparedness/Crisis-Management/COVID-19-Response/Pages/default.aspx]; provides (APHL member) access to COVID-19 Laboratory and Testing Resources including sample HL7 messages.

- International Association of National Public Health Institutes (IANPHI), COVID-19 Resources for Members and Global Public Health Professionals [https://ianphi.org/news/2020/covid-resources.html]; provides a summary of COVID-19 guidance from National Public Health Institutes world-wide.

- U.S. Centers for Disease Control and Prevention (US CDC), COVID-19 Information Management Resources (VADS) [https://phinvads.cdc.gov/vads/SearchVocab.action]; provides COVID-19 information to include public health reporting, laboratory reporting, case tracing/surveillance, and geo-spatial data exchange resources.

Annexure 11: Cloud and Shared Services References

- U.S. National Institutes for Science and Technology (NIST), *SP 800-145, The NIST Definition of Cloud Computing*, Peter Mell & Tim Grance, September 2011 [https://csrc.nist.gov/publications/detail/sp/800-145/final]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3500, *Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks* / Information technology - Cloud computing - Overview and vocabulary, August 2014 [https://www.itu.int/rec/T-REC-Y.3500/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3501, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Framework and high level requirements, June 2016 [https://www.itu.int/rec/T-REC-Y.3501/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3502, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Information technology - Cloud computing - Reference architecture, August 2016 [https://www.itu.int/rec/T-REC-Y.3502/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3505, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Overview and functional requirements for data storage federation, May 2018 [https://www.itu.int/rec/T-REC-Y.3505/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3506, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Functional requirements for cloud service brokerage, May 2018 [https://www.itu.int/rec/T-REC-Y.3506/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3507, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Functional requirements of physical machine, December 2018 [https://www.itu.int/rec/T-REC-Y.3507/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3508, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Overview and high-level requirements of distributed cloud, August 2019 [https://www.itu.int/rec/T-REC-Y.3508/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3509, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Functional architecture for data storage federation, December 2019 [https://www.itu.int/rec/T-REC-Y.3509/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3510, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing infrastructure requirements, February 2016 [https://www.itu.int/rec/T-REC-Y.3510/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3512, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Functional requirements of Network as a Service, August 2014 [https://www.itu.int/rec/T-REC-Y.3512/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3513, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Functional requirements of Infrastructure as a Service, August 2014 [https://www.itu.int/rec/T-REC-Y.3513/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3515, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Functional architecture of Network as a Service, July 2017 [https://www.itu.int/rec/T-REC-Y.3515/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3517, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Overview of inter-cloud trust management, December 2018 [https://www.itu.int/rec/T-REC-Y.3517/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3519, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing - Functional architecture of big data as a service, December 2018 [https://www.itu.int/rec/T-REC-Y.3519/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3522, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / End-to-end cloud service lifecycle management requirements, December 2018 [https://www.itu.int/rec/T-REC-Y.3522/en]

- ITU-Telecommunications Standardization Sector of the ITU, Recommendation ITU-T Y.3524, *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities* / Cloud computing maturity requirements and framework, December 2019 [https://www.itu.int/rec/T-REC-Y.3524/en]

- ITU-Telecommunications Development Sector, *Cloud Computing in Africa Situation and Perspectives*, April 2012 [http://www.itu.int/ITU-D/treg/publications/Cloud_Computing_Afrique-e.pdf]

- European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 - 0050 [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046]

- U.S. H.R.4943 - Cloud Act, 115th Congress (2017-2018) [https://www.congress.gov/bill/115th-congress/house-bill/4943]

Annexure 12: Capacity Building References

- Africa CDC, *Framework for Public Health Workforce Development, 2020-2025*, 10 March 2020 [https://africacdc.org/download/framework-for-public-health-workforce-development-2020-2025/]

Annexure 13: Core Values and Principles Guiding the Development of the HIE Guidelines and Standards

The AU Member States HIE guidelines and standards framework has the following as guiding principles:

I) Solidarity and cooperation

Solidarity among the African Union Member States; Cooperation between the Africa Union Commission (AUC), Regional Economic Communities (RECs), African Institutions and International organizations; commitment by all the AU Member States towards achieving the International Health Regulations (IHR), Agenda 2063, African Continental free trade area agreement (AFCFTA) and the Sustainable Development Goals (SDGs) where data sharing is a critical component towards their realization.

II) Comprehensive

Adopting an ecosystem approach that is comprehensive in defining and applying the requisite elements and foundations to transform the health sector and make the continent better prepared for pandemics.

III) Transformative

Fully leverage, harness and accelerate impact on society by accelerating digital and data sharing through the development of this health information exchange guidelines and standards.

IV) Inclusive

Digital Transformation for AU Member States that is affordable and ubiquitous, creating equal access to opportunities and mitigating risks of exclusion.

V) Homegrown

VI) It will be led and owned by Africa's institutions, embedded in African realities, and will unleash the African spirit of creativity and innovation to generate homegrown technology adoption and solution development, while embracing what is good and relevant without reinventing the wheel. TheAfrican experts led the development of this guidelinespolicy and standards document for African use.

VII) New Mindset

Benefiting from the digital transformation necessitates a shift in mindset as well as new forms of collaboration among stakeholders and across sectors, as well as facilitation and retooling. With the rapid evolution of technology and infrastructure, sharing data at the continental level will necessitate an open mind and a willingness to try something new..

VIII) Safe

IX) While balancing data sharing requirements, privacy and security of health data are high priorities. This document accomplishes a balance between privacy, security, and data sharing requirements.

X) Innovative

This HIE guidelinespolicy and standards framework tries to take advantage of the latest innovations in health information exchange by bringing the global experiences to Africa while still leaving room for more development and growth.

Annexure 14: Data Sharing and Use Agreement Template

DATA SHARING AND USE AGREEMENT

BETWEEN

[AFRICA CDC]

AND

[REQUESTING ORGANIZATION NAME]

This Data Sharing Agreement (hereinafter referred to as this 'Agreement') is entered into by and between the African Union (hereinafter referred to as the "AU"), acting through the Africa Centres for Disease Control and Prevention (hereinafter referred to as the "Africa CDC") whose principle address is at the African Union Headquarters P.O. Box 3243, Roosevelt street W21K19, Addis Ababa, Ethiopia on one part; and ABCD[1] (hereinafter referred to as the "ABCD") whose principle address is ……………………………. on the other part;

HEREINAFTER collectively referred to as the "Parties" and individually as the "Party" to this Data sharing Agreement.

WHEREAS the Africa CDC is a specialized technical institution of the African Union charged with the responsibility of promoting the prevention and control of diseases in Africa, in particular through its New Public Health Order strategy which calls for: (i) expanded manufacturing of vaccines, diagnostics, and therapeutics, (ii) strengthened public health workforce, (iii) respectful action-oriented partnerships, (iv) domestic Financing and (v)strengthened public health institutions.

WHEREAS ABCD has a mandate to ……………….;

WHEREAS Article 5(3) (a-d) of the Africa CDC Statute emphasizes that Africa CDC shall facilitate easy access to critical information that prepares and supports countries to respond to public health events;

WHEREAS "ABCD" has approved to share Data with Africa CDC, and "ABCD" has approved Africa CDC to use the shared Data to inform its actions for "ABCD" and the continent as part of its mandated function and to enable Africa CDC fully perform its responsibilities which is set out in Appendix C.

WHEREAS Africa CDC and "ABCD" mutually agree to enter into this Agreement to comply with the requirements of the national public health agency, Research Ethics Committee and National Health Research Authority policies and procedures for the transfer, handling, storage, and management of Data provided to Africa CDC from "ABCD" to the extent that those policies and procedures apply, and to comply with the ………………….;

WHEREAS the Data (hereinafter "Data" shall be collected from ……………………….

[1] The ''ABCD'' should be replaced by the name of the responsible institution in the Member State

NOW, THEREFORE, in consideration of the foregoing and any other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. *Term*

Unless otherwise terminated as provided herein, this Data Sharing Agreement will commence on the last date of signature by the Parties as indicated by the signature of the duly authorized representative of the Parties.

2. *Purpose*

The purpose of this Agreement is for "ABCD" to share all public health related information to enable Africa CDC to fully carry out its mandated function of using accurate and timely Data to inform action for African Union Member States.

3. *Definitions*

"Applicable law" refers to International Law to which AU is subject to and the applicable laws, regulations and requirements having the force of law, in the jurisdictions in which the Data originates and where the project is being performed to the extent, they are applicable to the matter and activities contemplated in this Agreement, and provided that the latter does not contravene with International Law.

"Data" shall refer to all communicable and non-communicable, endemic, epidemic, emerging and re-emerging diseases from national public health institutions or other relevant departments (e.g. laboratories, public health surveillance departments, emergency preparedness and response divisions, disease prevention and control divisions.

"Data quality" shall refer to Data and information that meet specific criteria to be fit for their intended use. In public health, the most desired characteristics of Data quality are completeness, timeliness, and accuracy.

"Public Health related Information refers to public health research data and products, public health policies, strategies, guidelines, standard operating procedures, information of health administration and human resource.

4. Data Transfer

4.1 "ABCD" will share de-identified Data with Africa CDC and may share identifiable Data where such information is critically needed to guide Africa CDC response efforts for "ABCD" or the continent. Africa CDC will follow a secure file transfer protocol or similar service of exchange as will be agreed by both Parties.

4.2 The Parties agree that technology such as secure File Transfer Protocol (sFTP) or similar service will be utilized. "ABCD" will work with Africa CDC prior to Data transfer to determine specific protocols, credentials, and transmission requirements/alternatives as per the laws of the African Union and "ABCD"

4.3 The Parties agree that "ABCD" accepts responsibility for the security of the information until it is received by Africa CDC as per the agreed method.

4.4 The Parties agree that Africa CDC has secured servers to host the Data and has developed a Data management system which shall host the Data and serve as an analytic platform for Data shared, respectively.

4.5 Africa CDC shall consult "ABCD" prior to the Data transfer to determine the specific protocols, credentials, and transmission requirements/alternatives consistent with the Law governing the African Union or/and "ABCD".

4.6 Africa CDC will use the "ABCD" Data only for the purposes of safeguarding the health of the MS and Continent including generation of reports and joint publications in scientific journals. Africa CDC shall not share the Data outside of the African Union Commission.

4.7 Africa CDC is not authorized to use or disclose the Data in a manner that would violate any clause stated in this agreement including the confidentiality and privacy of any identifiable Data.

5. Data Quality, Exchange Architecture and frequency

5.1 "ABCD" shall take responsible steps to ensure Data reported is of high quality.

5.2 The Parties agree that all Data shall be exchanged at the national level with the authorized institution (s) of "ABCD". Data in Africa CDC repositories shall be partitioned to allow Parties to control their own digital health Data and the timing of any subsequent release of that Data.

5.3 The Parties agree that the Data shall be sent to Africa CDC and once received, the Data shall be accessed by Africa CDC and the "ABCD" in accordance with this Agreement.

5.4 "ABCD" shall share all information and Data on International Health Regulation notifiable diseases and events for immediate reporting with Africa CDC. This Data shall be shared within 24 hours of detection.

5.5 All information related to disease outbreaks including but not limited to the following Data types: laboratory, case management, surveillance, risk communication and response Data shall be shared daily. ABCD shall share information on all other diseases and events weekly with the Africa CDC. All other public health related information shall be shared immediately as they become available or an update is made to an existing version.

6. Information Safeguards.

6.1 In the performance of the obligations under this Agreement, Each Party will adopt and use appropriate administrative, physical, and technical safeguards to preserve the integrity and confidentiality of the Data and to prevent its use or disclosure, other than as permitted by this Agreement or as required by laws on Data and privacy protection.

6.2 However, there shall be no obligation of confidentiality or restriction on the use of Data where:

i. The Data is publicly available, or becomes publicly available otherwise than by action of the receiving Party; or

ii. The Data was already known to the receiving Party (as evidenced by its written records) prior to its receipts.

iii. The Data was received from a third Party not in breach of any obligation of Confidentiality

6.3 Except to the extent required by law, neither Party will be responsible for ensuring that the other Party is taking necessary measures to comply with such applicable laws. Africa CDC may request from "ABCD" a copy of its privacy and access to Data policy in order to determine the controls in place and measures to ensure compliance with the Applicable laws relating to Data protection and privacy.

7. Publications

7.1 The Africa CDC shall appropriately attribute the provision of the Data in any resulting publications or oral presentations of the Data, in accordance with the acknowledgement(s) set out below. Named authors shall be determined in accordance with generally accepted publication standards and MS policies.

7.2 Before any Party submits a paper or abstract for publication or otherwise publicly discloses information regarding the Data, the Party that wishes to publish shall ensure the other Party has at least thirty (30) days to review the proposed publication or disclosure and that the comments provided shall be acted upon in good faith. In absence of any objection by the receiving Party within a thirty (30) day period concerning the prejudice to its proprietary rights, the Party that wishes to publish shall proceed with the publication.

8. Intellectual Property

8.1It is expressly agreed that neither "ABCD" nor Africa CDC transfers by operation of this Agreement to the other Party any right in or license to any patents, copyrights, or other proprietary right owned as of the commencement date of the Agreement or arising outside of the research conducted under this Agreement. All other information, work, copyrights, patents, trade secrets, or other intellectual property rights associated with any procedures, workflow, methods, reports, manual, visual aids, documentation, ideas, concepts, techniques, visuals, processes, articles, papers, or other works of authorship developed, provided that it was created by Africa CDC, during the course of this Agreement shall be owned by Africa CDC. Both Parties acknowledge that "ABCD" retains ownership of the Data.

8.2The terms of this section and sub-parts survive the termination, expiration, non-renewal, or rescission of this Agreement.

9. Compliance

Both "ABCD" and Africa CDC agree to use Data and otherwise to perform this Agreement in compliance with all applicable laws, regulations, policies, and policies of their respective institutions, including without limitation to those relating to human subjects. As appropriate, both "ABCD" and Africa CDC shall comply with applicable laws and regulations, as amended from time to time, with the respect to the collection, use, storage and disclosure of any Data, including without limitation.

10. Notice

10.1 Any notice required under this Agreement shall be in writing and shall be delivered personally or sent by the registered or certified mail, facsimile to the addresses listed below or such other addresses as either Party shall have notified the other Party.

To African Union:

The Director
Africa CDC
African Union
P.O. Box 3243
Addis Ababa
Ethiopia

To "ABCD":

10.2 Either Party may, by notice in writing to the other Party, designate additional representatives or substitute other focal points for this designated in this Article.

11. Termination

11.1 Termination for Cause. In the event that Africa CDC has breached a material term of this Agreement and fails to cure such breach within thirty (30) days after receipt of a written notice from "ABCD". "ABCD" shall be entitled to terminate the Agreement upon thirty (30) days prior written notice to the Party in breach and shall request Africa CDC to return of all Data.

11.2 Termination for Convenience. This Agreement may be terminated by either "ABCD" or Africa CDC giving to the other Party a minimum of thirty (30) days prior written notice, subject to the orderly conclusion of any ongoing activities and the settlement of outstanding obligations.

11.3. Continuing Privacy Obligations. The obligation of each Party to protect the privacy of the participants whose Data is the subject of this Agreement is continuous and survives any termination, cancellation, expiration, or other conclusion of this Agreement or any other agreement between Parties.

12. Destruction and Return of Data.

12.1. Africa CDC shall archive all Data received from "ABCD" and shall destroy any Data received upon request from "ABCD". Africa CDC will maintain the privacy of Data sets with personal identifiers to preserve the integrity of the Data sharing process.

13. Continuing Privacy Obligations.

Africa CDC's obligation to protect the privacy of the Data is continuous and survives any termination, cancellation, expiration, or other conclusion of this Agreement with respect to any portion of the Data, Africa CDC maintains after such termination, cancellation, expiration or other conclusion of this Agreement.

14. Use of Name

Neither Party shall use the names or trademarks of the other Party or of any of the other Party's affiliated entities in any advertising, publicity, endorsement, or promotion unless the other Party has provided prior written consent for the particular use contemplated. The terms of this section survive the termination, expiration, non-renewal, or rescission of this Agreement.

15. Status of Parties

Nothing in this Agreement shall be deemed or construed to create an employment, joint venture, or agency relationship between "ABCD" and Africa CDC. Neither "ABCD" nor Africa CDC shall have the authority to make any statements, representations or commitments of any kind, or to take any action, which shall be binding on another Party, without the prior written authorization of the other Party.

16. Warranty Disclaimer and Limitation of Liability

16.1 NEITHER PARTY MAKES ANY REPRESENTATIONS OR WARRANTIES, EXPRESSED OR IMPLIED, REGARDING ITS PERFORMANCE UNDER THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO, THE MARKETABILITY, USE OR FITNESS FOR ANY PARTICULAR PURPOSE OF THE DATA DEVELOPED AND SUPPLIED UNDER THIS WORK, OR THAT SUCH DATA DO NOT INFRINGE UPON ANY THIRD-PARTY PROPERTY RIGHTS. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER HEREUNDER FOR SPECIAL LOSSES, CONSEQUENTIAL, INCIDENTAL, OR OTHER INDIRECT DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT.

16.2 "ABCD" and Africa CDC agree to be responsible for their own wrongdoing, negligence and/or reckless acts or omissions in the performance of their duties hereunder and shall be financially and legally responsible for all of their expenses, liabilities, and attorney fees resulting from or attributable to any such acts or omissions. Neither Party shall have an obligation to indemnify the other hereunder. The terms of this paragraph shall survive expiration of this Agreement.

17. No Assignment

Neither Party may assign its rights hereunder to any third Party without the prior written consent of the other Party; provided, that a Party may assign its rights without the prior written consent of the other Party to any affiliate or other entity that controls, is controlled by or is under common control with such Party. Any purported assignment in violation of this clause is void. Such written consent, if given, shall not in any manner relieve the assignor from liability for the performance of this Agreement by its assignee.

18. Binding Effect

This Agreement shall be binding on both Parties upon and inure to the benefit of the Parties, legal representatives, successors and assigns.

19. Dispute Resolution

The Parties shall make every effort to resolve any disputes amicably and through diplomatic channels.

20. The Governing Law

This agreement shall be governed by International Law.

21. Privileges, Immunities and Facilities of Both Parties

Nothing in this Agreement shall be interpreted or construed as a waiver or a modification of the privileges, immunities and facilities, which the African Union enjoys by virtue of the international agreements and laws applicable to the Parties.

22. Severability

If any provision of this Agreement is held to be invalid or unenforceable, such provision shall be severed and the remainder of the provisions shall remain in full force and in effect as if this Agreement has been executed with the invalid provision eliminated. If any provision of this Agreement is so found to be invalid or unenforceable but would be valid or enforceable if some part of the provision were deleted, the provision in question shall apply with such modification as may be necessary to make it valid.

23. Entire Agreement, waiver, amendment

The Parties to this Agreement may not amend, alter or modify except by written agreement or exchange of letters signed by both Parties. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving Parties. A waiver of any term or provision shall not be construed as a waiver of any other term or provision. This Agreement constitutes the final, complete and exclusive agreement between the Parties with respect to its particular subject matter only (the sharing of de-identified Data) and supersedes all past and contemporaneous agreements, promises, and understandings, whether oral or written, between the Parties.

24. Counterparts

This Agreement may be executed in any number of counterparts, each of which, when executed and delivered (which may be delivered by way or an email), shall constitute one original, and photocopy, facsimile, electronic or other copies shall have the same effect for all purposes as an ink-signed original. Each Party hereto consents to be bound by photocopy or facsimile signatures of such Party's representative hereto.

IN WITNESS WHEREOF, the undersigned being duly authorised for this purpose by the respective Parties, have signed this Data Sharing Agreement.

Done at [……………………], [………………] on this ……. day of …………….. .

SIGNATURES APPEAR ON THE NEXT PAGE

“ABCD”_________________________________

By: _______________________________

Name: ______________________________

Title: _______________________________

Date:________________________________

African Union

By: _______________________________

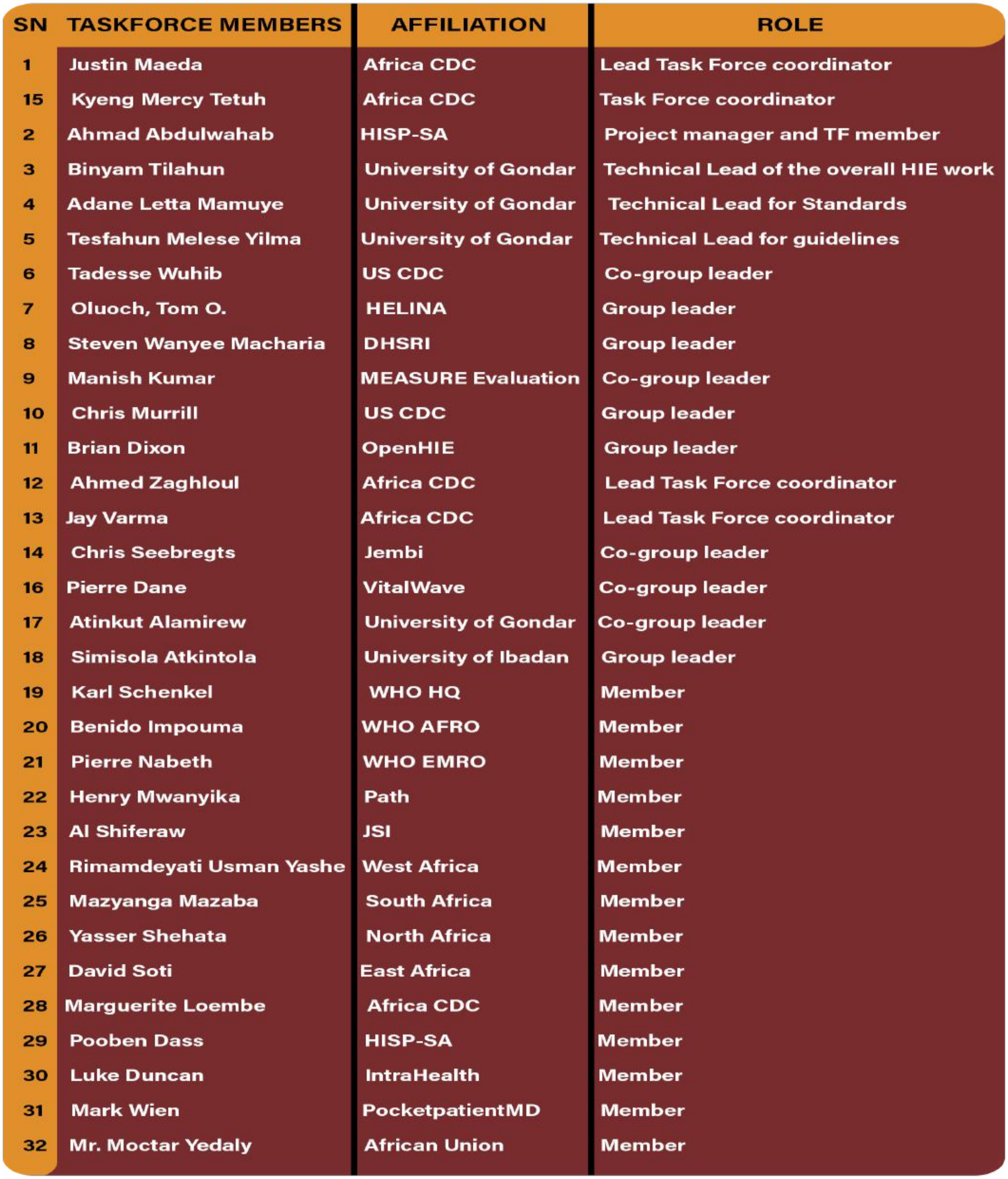
Name: ______________________________

Title: _______________________________

Date:________________________________

Annexure 15: List of Task Force Members and Contributors

Table 15. Task Force Members and Contributors



SN	TASKFORCE MEMBERS	AFFILIATION	ROLE
1	Justin Maeda	Africa CDC	Lead Task Force coordinator
15	Kyeng Mercy Tetuh	Africa CDC	Task Force coordinator
2	Ahmad Abdulwahab	HISP-SA	Project manager and TF member
3	Binyam Tilahun	University of Gondar	Technical Lead of the overall HIE work
4	Adane Letta Mamuye	University of Gondar	Technical Lead for Standards
5	Tesfahun Melese Yilma	University of Gondar	Technical Lead for guidelines
6	Tadesse Wuhib	US CDC	Co-group leader
7	Oluoch, Tom O.	HELINA	Group leader
8	Steven Wanyee Macharia	DHSRI	Group leader
9	Manish Kumar	MEASURE Evaluation	Co-group leader
10	Chris Murrill	US CDC	Group leader
11	Brian Dixon	OpenHIE	Group leader
12	Ahmed Zaghloul	Africa CDC	Lead Task Force coordinator
13	Jay Varma	Africa CDC	Lead Task Force coordinator
14	Chris Seebregts	Jembi	Co-group leader
16	Pierre Dane	VitalWave	Co-group leader
17	Atinkut Alamirew	University of Gondar	Co-group leader
18	Simisola Atkintola	University of Ibadan	Group leader
19	Karl Schenkel	WHO HQ	Member
20	Benido Impouma	WHO AFRO	Member
21	Pierre Nabeth	WHO EMRO	Member
22	Henry Mwanyika	Path	Member
23	Al Shiferaw	JSI	Member
24	Rimamdeyati Usman Yashe	West Africa	Member
25	Mazyanga Mazaba	South Africa	Member
26	Yasser Shehata	North Africa	Member
27	David Soti	East Africa	Member
28	Marguerite Loembe	Africa CDC	Member
29	Pooben Dass	HISP-SA	Member
30	Luke Duncan	IntraHealth	Member
31	Mark Wien	PocketpatientMD	Member
32	Mr. Moctar Yedaly	African Union	Member

African Union

AFRICA CDC
Centres for Disease Control and Prevention
Safeguarding Africa's Health

Africa Centers for Disease Control and Prevention (Africa CDC),
Africa Union Commission
Roosevelt Street W21 K19, Addis Ababa, Ethiopia

☎ +251 11 551 7700 www.africacdc.org ✉ africacdc@africa-union.org africacdc @AfricaCDC