DIGITAL HEALTH ENTERPRISE ARCHITECTURE, STANDARDS AND KNOWLEDGE PRODUCTS

A Guide to Standardising Digital Health in Uganda's Health System

April, 2023

TABLE OF CONTENTS

TABLE OF CONTENTS ii
LIST OF ACRONYMS iv
LIST OF FIGURES v
LIST OF TABLES vi
FOREWORD vii
PREFACE viii
ACKNOWLEDGEMENTS ix
THE RESEARCH TEAM x
EXECUTIVE SUMMARY xii
INTRODUCTION 1
SECTION 1: DIGITAL HEALTH ENTERPRISE ARCHITECTURE 3
COMPONENT 1: DIGITAL HEALTH ARCHITECTURE VISION AND GOALS 4
COMPONENT 2: DIGITAL HEALTH ARCHITECTURE GOALS 6
COMPONENT 3: MoH INFORMATION MANAGEMENT PRINCIPLES 7
COMPONENT 4: ARCHITECTURE PROCESS 19
COMPONENT 5: DIGITAL HEALTH MONITORING & EVALUATION 28
COMPONENT 6: DH ENTERPRISE ARCHITECTURE GOVERNANCE MODEL 32
COMPONENT 7: DIGITAL HEALTH SECURITY ARCHITECTURE 42
Section 2: DIGITAL HEALTH STANDARDS FOR UGANDA 48
2.1. Data and Interoperability Standards 48
2.2 DIGITAL HEALTH Communication Infrastructure Standards 53
2.2.1. HARDWARE DEVICES STANDARDS 54
2.2.2. COMMUNICATION NETWORKS & CONNECTIVITY STANDARDS 56
2.2.3. APPLICATION, SOFTWARE AND TECHNOLOGIES STANDARDS 60
2.2.4. DHCI's FACILITATING RESOURCES STANDARDS 61
2.2.5. SECURITY AND PRIVACY STANDARDS 64
Section 3: DH WORKFORCE CAPACITY BUILDING FRAMEWORK 67
DH Competency Model 67
DHW JOB ROLES AND REQUIRED PROFICIENCIES 67
Proficiency Levels required for Digital Health Worker (DHW) in Uganda 67
CONCLUSION 69
REFERENCES 70
APPENDICES 73
APPENDIX A.1 STANDARDISATION FRAMEWORK 73
APPENDIX A.2: STANDARDISATION PROCESS 74

APPENDIX B.1: USE CASE – HIV/TB Client Management System Architecture For IDI Clinic, Mulago 75

APPENDIX B.2: Use Case – Contextualising Terminology Codes for HIV Disease Management Services 81

APPENDIX C.1: DH Monitoring & Evaluation indicators and operationalisation tools. 86

APPENDIX C.2: Results chain based on the results-based management strategy 89

APPENDIX C.3: Categorisation of DH Indicators 89

LIST OF ACRONYMS

DH	Digital Health
DH-ASK	Digital Health Architecture, Standards and Knowledge Products
DHEAF	Digital Health Enterprise Architecture Framework
DHIM	Division of Health Information Management
DHM&EF	Digital Health Monitoring and Evaluation Framework
eHealth	Electronic Health
HIE	Health Information Exchange
HIIRE	Health Information and Innovation Research
HIV	Human Immunodeficiency Virus
HSE	Health Sector enterprise
IDI	Makerere University Infectious Disease Institute
ISO	International Organisation for Standardisation
ICT	Information and Communication Technology
ITU	International Telecommunications Union
LMIC	Low- and Middle-Income Country
MoH	Ministry of Health
MoICT	Ministry of Information and Communication Technology
NITA-U	National Information Technology Authority - Uganda
PEPfAR	U.S. President's Emergency Plan for AIDS Relief
SDG	Sustainable Development Goals
WHO	World Health Organisation

LIST OF FIGURES

Figure 1. Digital Health Enterprise Architecture Framework 3
Figure 2. Digital Health Enterprise Architecture Framework for Uganda 4
Figure 3. Digital Health Architecture Vision for Uganda 5
Figure 4. EA requirements, Outcomes, and Goals Model 7
Figure 5. Architecture Process 20
Figure 6. Digital Health Evaluation Reference Model 29
Figure 7. Digital Health Governance structure 33
Figure 8. Architecture Policy Development Process 38
Figure 9. Architecture Compliance Review Process 38
Figure 10. MoH Architecture Repository 42
Figure 11. Digital Health Information Security Architecture 43
Figure 12. Data Standards 48
Figure 13. Standards for DHCI 53
Figure 14. Framework for Standardisation of Uganda's Digital Health Interventions 73
Figure 15. Process of selecting suitable standards for Digital Health 74
Figure 16: Goals, objectives, and requirements relationship diagram 76
Figure 17. Modelling Language for HIV/TB Client Management System Architecture 79
Figure 18. Symbols used in the CMS Architecture 79
Figure 19. Integrated HIV/TB Client Management System Model (Initial version) 80
Figure 20. Process of Contextualising Health Terminologies 81

LIST OF TABLES

Table 1. Digital Health Enterprise Architecture Goals for Uganda 6
Table 2. HSE Enterprise Principles 8
Table 3. MoH Business Architecture Principles 10
Table 4. MoH Data Architecture Principles 13
Table 5. MoH Application Architecture Principles 15
Table 6. Digital Health Technology Architecture Principles 16
Table 7. MoH Interoperability Principles 17
Table 8. MoH Security and Privacy Principles 17
Table 9. Inputs and Outputs of Preliminary Phase 20
Table 10. Inputs and Outputs of Architecture Vision Phase 21
Table 11. Inputs and Outputs of Business Architecture Phase 21
Table 12. Inputs and Outputs of Data Architecture Phase 22
Table 13. Inputs and Outputs of Application Architecture Phase 23
Table 14. Inputs and Outputs of Technology phase 23
Table 15. Inputs and Outputs of Technology phase 24
Table 16. Inputs and Outputs of the migration planning phase 25
Table 17. Inputs and Outputs of Implementation Governance 26
Table 18. Inputs and Outputs of Architecture Change Management Phase 27
Table 19. Mapping Digital Health maturity stages with the results chain and Digital Health evaluation questions 30
Table 20. Example of Digital Health monitoring and evaluation reporting tool 31
Table 21. Proficiency Levels of DHWs 68
Table 22. IDI EA Requirements, Outcomes and Goals 75
Table 23. Assumptions, Potential Risks and Mitigation Measures 76
Table 25. provides the recommended coding standards that should be followed in the implementation of HIV/TB CMS. 78
Table 25. Recommended Semantic Standards to Support HIV/TB CMS 78
Table 26. Presents the guidelines for protecting and managing HIV/TB data. 78
Table 27. Use Case - Terminology Codes for HIV Disease Management Services 82

FOREWORD

The government of the Republic of Uganda recognises the use of information and communication technology (ICT) in the National Development Plan III 2020/21 - 2024/25 as an enabler to improve the delivery of services to its citizens across its sectors. The Ministry of Health Strategic Plan 2020/21 – 2024/25 also recognises eHealth as a key enabler for supporting the health system in order to deliver good health to the population. In addition, the National eHealth Policy 2016 provides guidance on how to use ICT to facilitate improvement in the flow of information, through electronic means, to support the delivery of health services and the management of the health system in a bid to facilitate universal access to care, health sector efficiency, and social transformation.

Currently, the government, partners, and private institutions have continued to invest in various ICT initiatives. However, there is lack of a national plan to coordinate the development of digital health interventions in the country; and hence, increasing the risk of continued duplication, fragmented/siloed systems that cannot be integrated or scaled across the continuum of care, data duplication, security and privacy of patients' data. Standardisation can be used to develop the standards requirements for Uganda's digital health in order to address such digital health challenges.

Consequently, this Standardisation guide presents several digital health artefacts that aim to standardise digitally-enabled healthcare and services in Uganda's health system including the Digital Health Enterprise Architecture that should define the "how and what" different digital health resources work together to optimise delivery of healthcare and services, as well as digital health Standards that aim to provide the common rules, principles, and guidelines for use and usage of various digital health interventions in Uganda's health system.

Hon. Dr. Jane Ruth Aceng Ocero (MP)
Minister of Health

PREFACE

The Ministry of Health recognises the potential of information and communication technology (ICT) in transforming healthcare delivery by enabling information access and supporting healthcare operations, management, and decision-making. However, Uganda's health sector is characterised by a fragmented and siloed landscape of digital health interventions/pilot projects with significant barriers to effective sharing and exchange of information within and across Uganda's health system. Although much of the data needed for clinical care, patient safety, and quality improvement resides on computers, there is no means to transfer the data easily and economically from one computer to another, despite the existence of such communications technologies to support such data exchange.

The key obstacle to achieving this capability is unavailability of data standards for organising, representing, and encoding clinical data/information so that the data can be understood and accepted by the receiving systems. At the health facility level, lack of common data standards has prevented information sharing for decision- and policy-making purposes and continuum of care. Lack of standards has also prevented reuse of clinical data to meet the broad range of patient safety and quality reporting requirements.

Accordingly, this Standardisation Guide provides a set of digital health artefacts (DH-ASK) that should guide standardisation of digitally-enabled healthcare and services in order to enhance health information management, and decision- and policy-making processes across the health sector. Production of Standardisation digital health artefacts was achieved through a participatory process spearheaded by Makerere University Health Informatics Research Group in collaboration with the Ministry of Health led by Dr. Sarah Byakika (Commissioner, Health Services, Planning, Financing and Policy), Division of Health Information (DHI) and the HIRE (eHealth) Technical Working Group. We extend our profound appreciation to each of the contributors to these DH-ASK artefacts for playing a key role in standardising digital health to strengthen Uganda's health system.

Dr. Diana Atwine
Permanent Secretary
Ministry of Health

ACKNOWLEDGEMENTS

The Ministry of Health expresses its profound gratitude to all departments and programs, members of the Health Information Innovation and Research (HIIRE) Technical Working Group, Digital Health Subcommittee, and the Health Data Collaborative subcommittee who contributed technical inputs leading to the successful completion of this document. Special appreciation goes to the Department of Planning, Financing and Policy for the overall guidance to ensure that the objectives of the Digital Health architecture, standards and knowledge products (DH-ASK) are aligned to the priorities of the NDP III and MoH Strategic Plan covering the 2021–2025 period. Special gratitude is also extended to the Makerere University Health Informatics Research Group for leading and collaborating in the research and development of the DH-ASK products, and the Makerere University Infectious Disease Institute (IDI) that provided the case study, as well as the study participants at the National and Sub-national levels who participated effectively in the study, development and validation of the DH-ASK products. Finally, I would like to acknowledge the Government of the Republic of Uganda through Makerere University Research and Innovation Fund (MakRIF) for sponsoring the research and development of the DH-ASK products; as well as thank all the development partners that provided financial and technical support for this process.

The Ministry of Health commits to the overall stewardship of these Digital Health architecture, standards and knowledge (DH-ASK) products through communication and dissemination, implementation, periodic monitoring and planned evaluations to assess and document successes, enablers and challenges.

Dr. Henry Mwebesa
Director General Health Services
Ministry of Health

THE RESEARCH TEAM

Principal Investigator

Dr. Josephine Nabukenya is a Professor of Information Systems & Health Informatics at the School of Computing and Informatics Technology, in the College of Computing and Information Sciences, Makerere University. She is a member of the Digital Health and Interoperability Working Group of Health Data Collaborative (HDC). She was part of the 10-member Core Team that developed the Uganda eHealth Policy and Strategy, and collaborates with the Ministry of Health for its implementation. She has over 20 years of research experience and a Principal Investigator and Collaborator on various Digital / Health Informatics / Information Systems / Health Systems research projects in Uganda, the Region and Globally.

Co-Investigators

Dr. Andrew Kambugu is the Sande-McKinnell Executive Director, Infectious Diseases Institute, College of Health Sciences, Makerere University and is an honorary Senior Lecturer in the Department of Medicine at MakCHS. He is a Fellow of the Royal College of Physicians (FRCP), London, UK. He is a principal investigator on a number of clinical trials spanning the fields of HIV therapeutics, HIV treatment strategies and implementation science in Uganda.

Dr. Mercy Rebekah Amiyo is a Lecturer at the School of Computing and Informatics Technology, College of Computing and Information Sciences, and Researcher in the Health Informatics Research Group, Makerere University. Her research interests focus on Information Systems, Business Process Management, Health Informatics and Data and Information Management.

Researchers

Andrew Alunyu Egwar is a PhD student in the Health Informatics Research Group, School of Computing & Informatics Technology, Makerere University. His research focuses on computer and data communications, standardisation of the digital health environment particularly the communication infrastructure that supports patient data sharing and health information exchange, securing patient data / health information in the eHealth system.

Moses Bagyendera is a PhD student in the Health Informatics Research Group, School of Computing & Informatics Technology, Makerere University. His research focuses on the Interoperability for data use and utilization in health care institutions in Uganda, as well as eHealth policy formulation, implementation and use in Africa and specifically at WHO.

Achilles Kiwanuka is a PhD student in the Health Informatics Research Group, School of Computing & Informatics Technology, Makerere University. He has carried out research on the adoption and standardisation of digital health technologies and systems. Currently, he is researching about how international eHealth medical coding standards can be contextualised to improve semantic interoperability in Uganda.

Joseph Wamema is a PhD student in the Health Informatics Research Group, School of Computing & Informatics Technology, Makerere University. His research is aimed at developing a digital health Enterprise Architecture Framework to streamline the digitalisation of Uganda's healthcare system. His research interests focus on the interoperability of digital health systems, barriers to successful adoption of digital health and the technology-fit of digital health in the African context.

Justus Ashaba is a researcher in the Health Informatics Research Group, School of Computing & Informatics Technology, Makerere University. His research interest focuses on the interplay of information systems and results-based management in the health sector particularly Monitoring and Evaluation frameworks to guide assessment of digital implementations and their impact and or outcomes in healthcare in Uganda and developing countries.

EXECUTIVE SUMMARY

The Standardisation Guide presents several digital health (DH) artefacts including; digital health Standards, digital health Enterprise Architecture Framework, digital health Workforce Capacity Building Framework, and digital health Monitoring and Evaluation Framework (DH-ASK). The DH-ASK artefacts will be used to standardise digitally-enabled healthcare and services in Uganda's health system.

Standardisation of the DH-ASK artefacts was derived from the requirements of an exploratory landscape study for digital health in Uganda's Health System. The landscape analysis provided an understanding of the challenges that impeded digital health standardisation and data-use-for-action in Uganda's health system. Whereas standardisation has been considered as a remedy to digital health challenges in many countries; conversely, the digital health standardisation ground is troubled with numerous challenges, including huge number of available standards, that compete, overlap and sometimes contradict one another; worse still, many of the available standards do not have implementation guidelines, which makes their implementation quite a difficult task. As such, adopting international digital health standards normally requires significant localisation to meet specific requirements of that country such as Uganda. Standardisation entails standards determination, implementation, compliance monitoring and review. Standardisation can be used to develop standards requirements for Uganda's digital health, with an aim to address digital health challenges such as fragmentation/siloed (un-interoperable) systems, data duplication, security and privacy of patients' data.

The digital health Enterprise Architecture Framework aims to define the "how and what" different digital health resources work together to optimise delivery of healthcare and services. The digital health Standards aim to provide the common rules, principles, and guidelines for use and usage of various digital health interventions in Uganda's health system. The digital health Monitoring and Evaluation Framework aims to assess results and impact of digital health interventions. The digital health Workforce Capacity Building Framework aims to define standardised digital health workers' skills, knowledge and appreciation of digital health in work practices.

INTRODUCTION

Standardisation has been considered as a remedy to digital health challenges in many countries (Adebesin et al., 2013; Adebesin & Kotzé, 2017; WHO & ITU, 2012). Conversely, the digital health standardisation ground is troubled with numerous challenges, including huge number of available standards, that compete, overlap and sometimes contradict one another (Alunyu & Nabukenya, 2018; Hammond, 2017; WHO & ITU, 2012); worse still, many of the available standards do not have implementation guidelines, which makes their implementation quite a difficult task (Alunyu & Nabukenya, 2018; MoH-Uganda, 2016). As such, adopting international digital health standards normally requires significant localization to meet specific requirements of that country such as Uganda. ***Standardisation*** entails standards determination, implementation, compliance monitoring and review (Costello & Parker, 2020; ISO/IEC, 2019; Kim & Matney, 2018). Standardisation can be used to develop standards requirements for Uganda's digital health, with an aim to address digital health challenges such as fragmentation/siloed (un-interoperable) systems, data duplication, security and privacy of patients' data.

Standardising digital health in Uganda was motivated by an exploratory landscape analysis of the digital health in Uganda's Health System (Alunyu et al., 2021; Kiwanuka et al., 2021; MoH-Uganda, 2021), that provided an understanding of the challenges that impeded digital health standardisation and data-use-for-action in Uganda's health system. The exploratory study used the HIV disease model to provide highlights of the state of art for digital health conducted in Uganda on grounds that several global and local interventions (i.e.; Uganda Government and Development Partners) as well as enormous investments had been made to control the epidemic (Ministry of Health-Uganda, 2010). Notably, PEPfAR sponsors 80% of the resources for Uganda's HIV response, which places great emphasis on the use of data-driven approaches to facilitate decision-making ensuring appropriate interventions are implemented in relevant populations in the right way (PEPfAR, 2019).

Principally, various, though duplicated and disintegrated data-driven digital health interventions have been developed in Uganda to manage the HIV epidemic. As such, patients' health data continues to be fragmented, unsecure and lacks privacy due to sitting on several siloed/un-interoperable digital health systems. This has greatly affected ease-of-use for such health data to inform patient care, clinical decision-making and policy-making. Worse still, the digital health interventions that have been successful in one healthcare program, are most times not integrate-able with others nor adopted by other similar programs within and across the same health system (i.e., these interventions may be useful in a specific health program).

In other words, their integration into a coherent national integrated health information system for Uganda is currently challenging.

Accordingly, to achieve a coherent National Integrated Digital Health Information System for Uganda, it would require standardisation for all digitally-enabled healthcare interventions; this is to facilitate their proper implementations to support health information exchange (HIE) within and across Uganda's health system. To this end, the contents of this Standardisation Guide report on several digital health (DH) artefacts including; digital health standards, digital health Enterprise Architecture Framework, digital health Worker Capacity Building Framework, and the digital health Monitoring and Evaluation Framework (DH-ASK). The DH-ASK artefacts aim to standardise digitally-enabled healthcare and services in Uganda's health system as stipulated in Uganda's Digital Health Policy and Strategy (2016/17-2020/21), other aligned policies/plans including Uganda's National Development Plan (2015/16–2019/20), Uganda Vision-2040; Health Sector Development Plan (2015/16–2019/20) on digital health development and implementation in Uganda; WHO global strategy on digital health (2020-2024) where standardising digital health is among the primary health systems strengthening building blocks; UN-SDG 3 to "ensure healthy lives and promote well-being for all at all ages", one of its targets being elimination of epidemics related to infectious diseases.

SECTION 1: DIGITAL HEALTH ENTERPRISE ARCHITECTURE

Enterprise Architecture (EA) is a description of an enterprise from an integrated business and IT perspective intended to bridge the communication gap between business and IT stakeholders and improve business and IT alignment (Kotusev, 2019; van de Wetering et al., 2021). This integrated view identifies and communicates the necessary improvements to business processes and IT assets to optimise an organisation's mission capabilities and resource utilization. EA, therefore, translates an organisation's vision and strategy into effective enterprise change by creating, communicating, and improving the key requirements, principles, and models that describe the enterprise's future state.

Figure 1 presents the Digital Health Enterprise Architecture Framework (DHEAF) for Uganda. This framework is intended to standardise the implementation of Digital Health across Uganda's health system by optimizing and transforming the often-fragmented processes, information, application systems, and technologies into an efficient and integrated environment supportive of Uganda's National eHealth strategy. The DHEAF, which comprises several components that work together, has been built on the foundations of the Uganda National eHealth Strategy 2017-2021 (MoH-Uganda, 2016). It is aligned with the Uganda e-Government Interoperability Framework (NITA-U, 2021), Uganda e-Government Interoperability Reference Architecture (GoU, 2021a), and Government of Uganda e-Government Web Application Security Architecture Framework (GoU, 2021b). This approach supports the alignment of the Ministry of Health Digital Health initiatives with the digital strategies of the Government of Uganda.

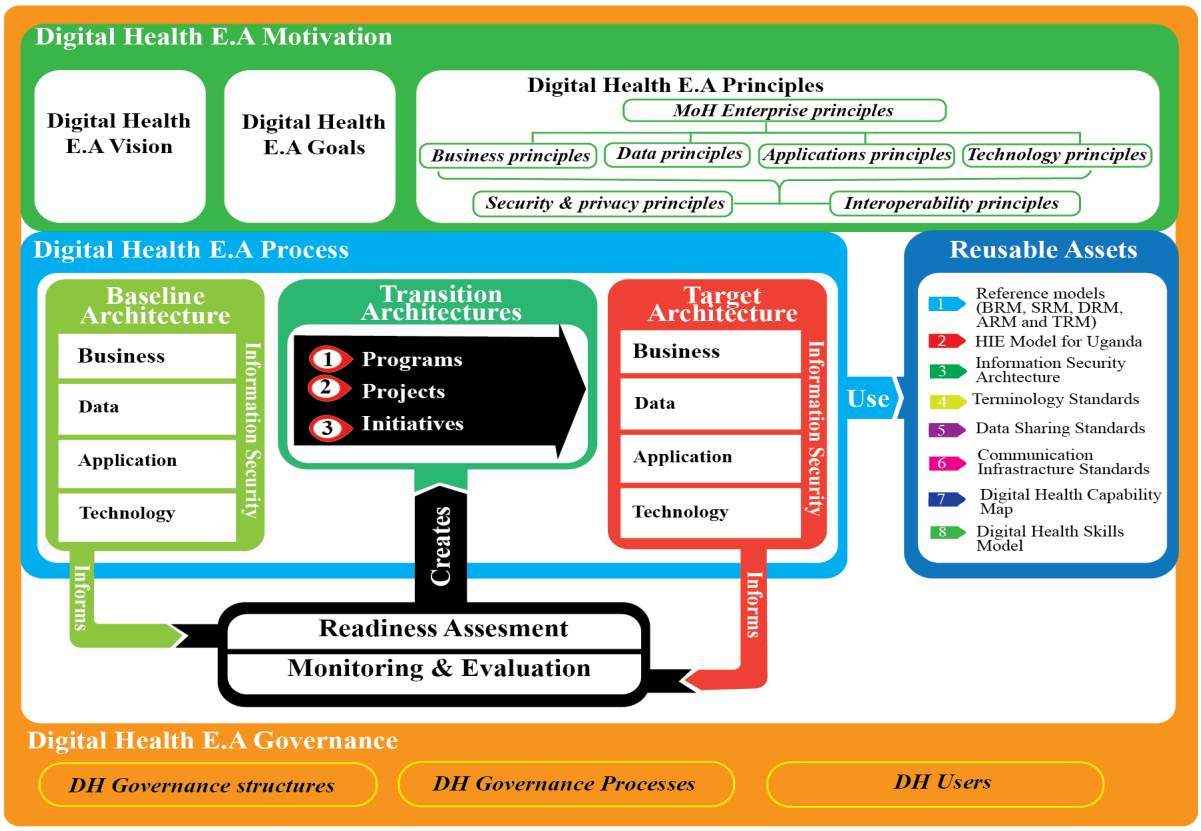


Figure 1. Digital Health Enterprise Architecture Framework for Uganda

The Digital Health Enterprise Architecture Framework (DHEAF) for Uganda is anchored on The Open Group Architecture Framework (TOGAF) version 9.2 and uses the semantic model for systems architecture defined in IEEE 1471-2000 standard. The DHEAF, incorporates best practices from several other popular Enterprise Architecture frameworks and standards, including; the Treasury Enterprise Architecture Framework (TEAF), California Enterprise Architecture Framework, Open Health Information Exchange Framework, and publications from the National Institute of Standards and Technology (NIST), Massachusetts Institute of Technology (MIT), National E-Health Transition Authority Limited (NEHTA) and Gartner.

DESCRIPTION OF DHEAF COMPONENTS

The DHEAF constitutes of seven building blocks/components that have to support each other to realise a standardised Digital Health environment where all stakeholders can seamlessly share health information. These building blocks/components are intended to reduce duplication, redundancies, and complexity as well as to promote shared Digital Health solutions while emphasising the security and privacy for health data.

COMPONENT 1: DIGITAL HEALTH ARCHITECTURE VISION AND GOALS

Digital Health Architecture Vision

An integrated foundation for Digital Health that ensures access to healthcare in a secure, transparent, efficient, and cost-effective manner in Uganda.

Description of EA Vision

Figure 2 and **Figure 3** illustrates the Digital Health Architecture Vision for Uganda. This vision, describes the dream for Uganda's health system target architecture, it is intended to create an integrated foundation for Digital Health that will ensure accessibility of healthcare in a secure, transparent, efficient, and cost-effective manner. It will serve as a model for all Health organisations that constitute Uganda's health system and will be a crucial input in all initiatives to create target architectures.

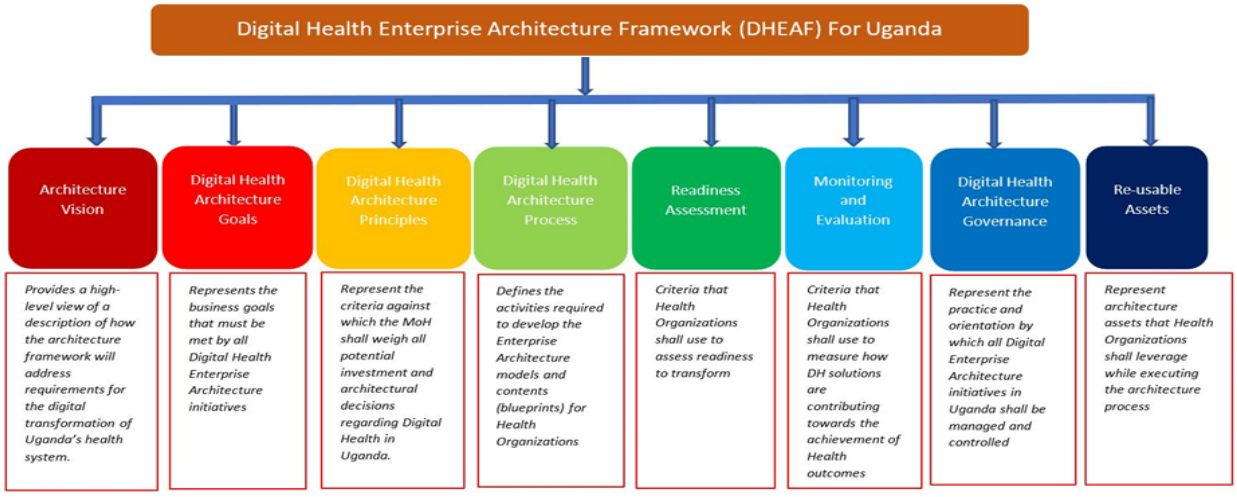


Figure 2. Description of the Eight Major Components of the Digital Health Enterprise Architecture Framework for Uganda

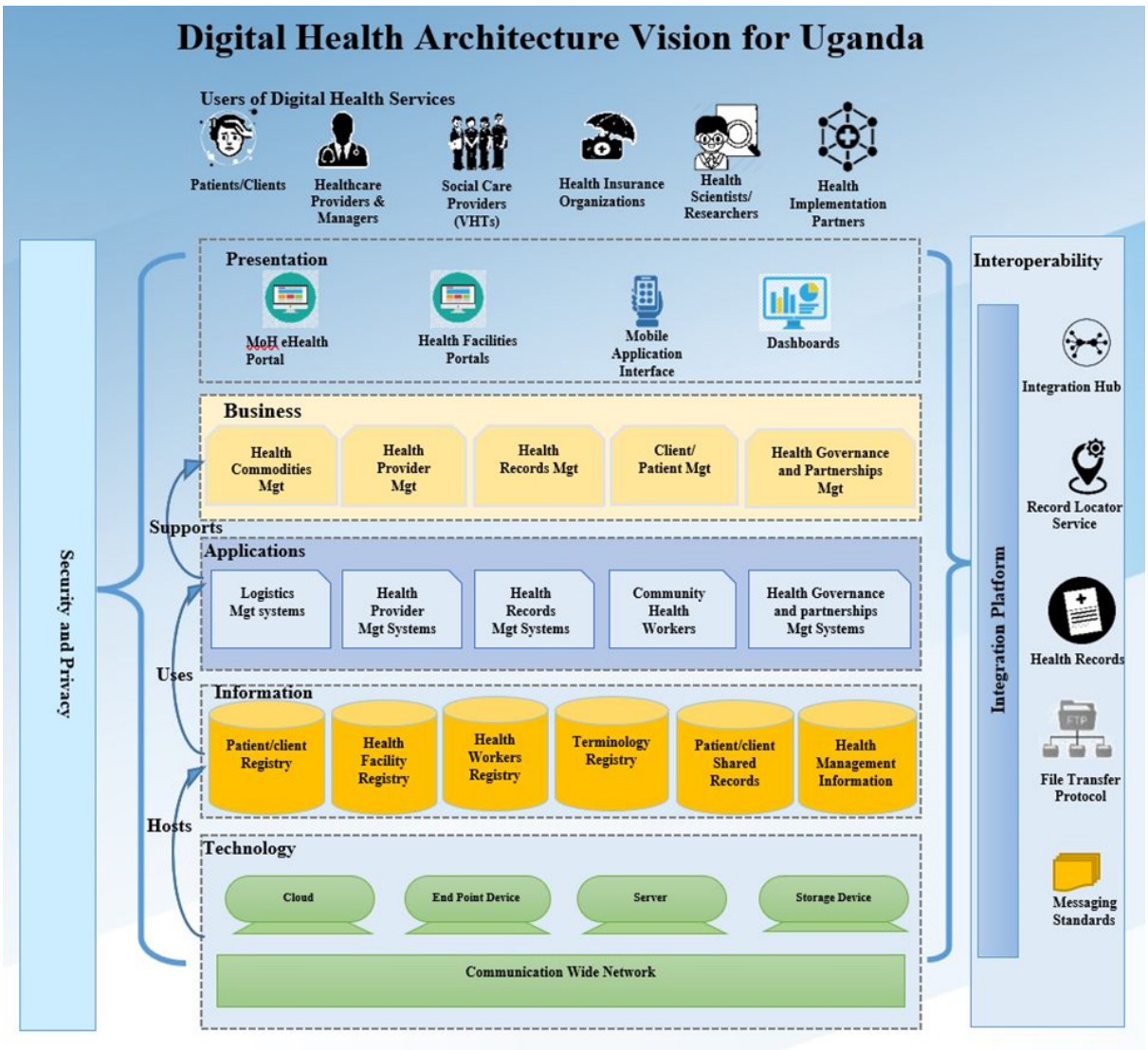


Figure 3. Digital Health Architecture Vision for Uganda (conceptualized based on TOGAF)

Digital Health users are categorised into six groups (including private healthcare organisations) and the supply chain as described hereunder:

- Patients/Clients – these are individuals that access health services
- Health Practitioners and Managers – these are individuals who are actively involved in either providing, supplying or overseeing the provision of health services
- Social Care Practitioners (VHTs) – these are individuals who deliver health support from the community to the health facility
- Health Insurance Organisations – these are organisations financing healthcare delivery through provision of insurance services
- Health Researchers – these are individuals and organisations involved in systematic investigations in the health sector
- Health Implementing Partners – these are organisations that support the Government of Uganda in implementation of health programs.

These users will access Digital Health services from the Ministry of Health (MoH) Portal, Health facility portal, Mobile Application Interfaces, and Dashboards. Health organisations shall be allowed to implement five major categories of Health Information Systems; Logistics Management systems, Health Provider Management systems, Health Records Management Systems, Community Health Worker systems, and Health Governance and Partnership Management systems. These systems shall be interoperable with Uganda's National Health Information Systems, such as DHIS2. To facilitate this, the DHEAF defines standards for integration. All Digital Health systems shall be required to conform to the standards before they are allowed to integrate with other health systems. Integration shall be through an interoperability platform.

The Integration Platform shall provide a single logical gateway into the core of the National Health Information System and standard-based channels for synchronous and asynchronous messaging between local Health Information Systems and the National Health Information System. Critical functions of the integration platform shall include security, messaging, and auditing. The MoH shall implement an integration platform through several specialized components, including; an Integration Hub, Resource Locator Service (RLS), File Transfer Protocol (FTP), and messaging standards.

This architecture vision also depicts five registries to support the management of health data, including; the Patient/Client, Health Facility, Health Worker, Terminology, Health Shared Record, and Health Management registries. In addition, datasets shall be normalised, integrated, and held centrally where necessary to support business capabilities. The detailed contents of these shall be driven by the information architecture and the detailed design of core applications and core services, the definition of which will continue to evolve and mature as the new Knowledge & Information capabilities are implemented. MoH shall host all Digital Health applications and registries in the cloud, endpoint devices, servers, and other storage devices as may be necessary. These will be linked together via a wide communication network.

To ensure the confidentiality, integrity, and availability of health data, Health organisations shall incorporate security governance in their everyday practices to effectively cope with the emerging security and privacy threats to health information. As such, security and privacy considerations must be factored into all the layers of the Uganda Health System, right from the technology layer to the application, data, and business layers. Security Governance must be integrated into Corporate Governance and regarded as a governance challenge that includes reporting, accountability, and adequate risk management.

COMPONENT 2: DIGITAL HEALTH ARCHITECTURE GOALS

The following business goals shall guide the implementation of the DHEAF for Uganda's Health System (See **Table 1**).

Table 1. Digital Health Enterprise Architecture Goals for Uganda

Business Goal	Notes
Business Goal 1	Harnessing Digital Health to facilitate transformation of Uganda's healthcare system and improve health outcomes

Business Goal 2	Making patient care safer and more effective by making available the correct information in the right place at the right time
Business Goal 3	To ensure equitable access to quality health services, with emphasis on improving access to health services by the underserved and vulnerable populations
Business Goal 4	To standardise the use of ICT in healthcare delivery to ensure interoperability of systems and timely access to health-related information
Business Goal 5	To safeguard confidentiality, privacy, and integrity of patient/client information

DIGITAL HEALTH ENTERPRISE ARCHITECTURE REQUIREMENTS, OUTCOMES, AND GOALS RELATIONSHIPS

Figure 4 shows the relationships that exists between the Enterprise Architecture requirements, outcomes, and goals model.

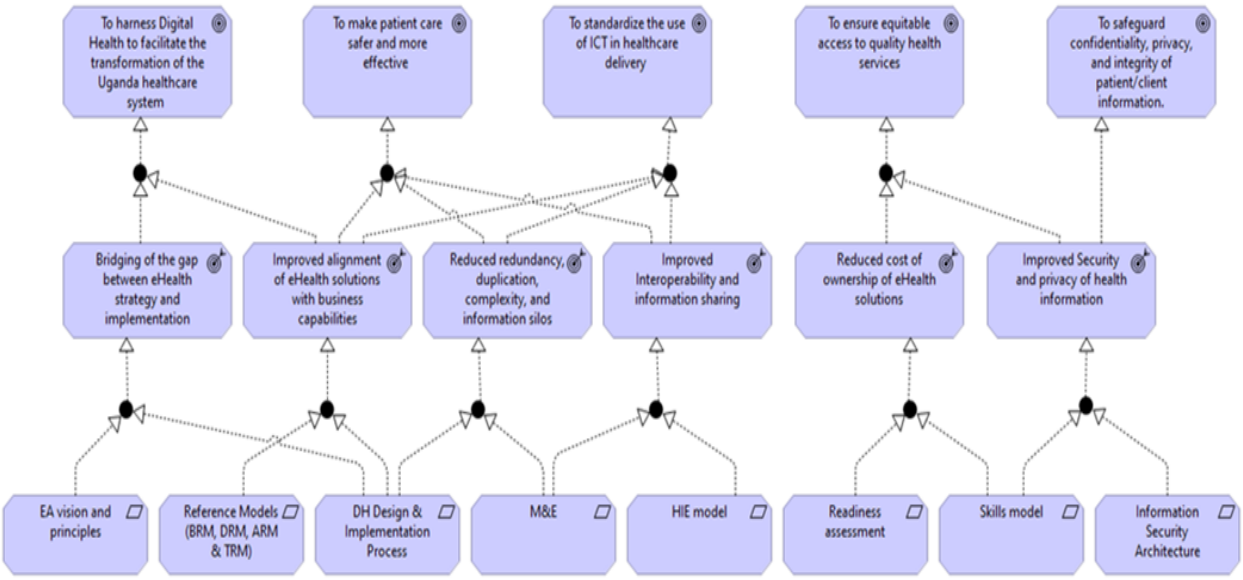


Figure 4. EA requirements, Outcomes, and Goals Model

COMPONENT 3: MoH INFORMATION MANAGEMENT PRINCIPLES

Principles are general rules and guidelines intended to be enduring and seldom amended that inform and support how an organisation fulfills its mission (Josey et al., 2018). Principles may be established within different domains and at different levels of an enterprise. This section presents the MoH Information Management principles that shall guide the implementation and use of Digital Health in Uganda. These principles are based on best practices from TOGAF, MIT, and NEHTA (Josey et al., 2018; NEHTA, 2012) and have been informed by:

- Uganda National eHealth Strategy (2017-2021)
- MoH Handbook on "Strengthening Uganda's Health System through Standardising Digital Health: Requirements for Digital Health Standards and Enterprise Architecture Framework" (2021)
- Legal and Regulatory Framework for Digital Health in Uganda
- Accepted architectural practices in the Information Technology industry

The MoH Information Management Principles are structured according to The Open Group Architecture Framework (TOGAF) recommendations. Each principle has a *Name* that highlights the essence of the principle, *a Statement* that unambiguously communicates the fundamental rule, a *rationale* that gives the business benefit of adhering to the principle, and *implications* that outline the critical tasks, resources, and potential costs associated with following the principle. The main objective of the MoH Information Management Principles is to support the delivery of Digital Health solutions that are interoperable, flexible, and fit-for-purpose while supporting established rules and processes for communication and the use of information within Uganda's health sector. These principles are divided into two, namely; enterprise principles and architecture principles.

Component 3A: MoH Enterprise Principles

Enterprise principles are general rules that provide a basis for decision-making throughout an enterprise and dictate how the organisation intends to fulfill its mission (Josey et al., 2018). Such principles are commonly used to harmonise decision-making at the strategic level and are a crucial element of the governance strategy. The four enterprise principles presented in **Table 2** shall guide decision-making at the strategic level of Uganda's Health System. Each principle has a code that reflects the category (i.e., Health Sector Enterprise (*HSE*) and the principle number (i.e., P1).

Table 2. HSE Enterprise Principles

CODE	**HSE-P1**
NAME	**Uganda's health sector is an integrated and dynamic enterprise**
STATEMENT	Uganda's health sector operates as a single enterprise with decision-making flexibility at National and sub-national levels
RATIONALE	A single enterprise with shared strategic objectives, joint governance, integrated management processes, and consistent policies improves the implementation of enterprise-wide strategies and the coordination of the delivery of health services to citizens
IMPLICATION	• Optimise resource allocations to achieve common goals across the entire health sector • Ensure availability and access to health information for evidence-based decision-making across the health sector • Digital Health architectural designs should integrate services for efficiency while keeping the autonomy of operations of the different units of the health sector
CODE	**HSE-P2**
NAME	**Improve the safety and quality of healthcare for citizens**
STATEMENT	Decisions about Digital Health must aim to improve the safety and quality of healthcare

RATIONALE	Providing safe, high-quality, and effective healthcare is a national priority. Digital Health investment decisions should support this priority and thus minimise healthcare risks associated with inaccurate and inadequate healthcare information and processes
IMPLICATION	• Apply applicable Institute of Medicine (IOM) quality principles of care to all decisions about Digital Health investments; that is, healthcare should be safe, effective, patient-centered, timely, and unbiased • Decisions about Digital Health investments should be driven by the need for safe, high-quality, effective healthcare rather than by technological or other external concerns
CODE	**HSE-P3**
NAME	**Improve the efficiency of healthcare services**
STATEMENT	Decisions about Digital Health investments should aim to improve the efficiency of healthcare service provision
RATIONALE	The provision of efficient healthcare is a national priority. Digital Health investment decisions should support this priority and thus improve the healthcare delivery processes.
IMPLICATION	• Decisions about Digital Health investments should be driven by the need for cost-efficient healthcare delivery rather than by technological or other external concerns • The applicable Institute of Medicine (IOM) quality of care principles should be applied to such decisions; that is, healthcare should be efficient
CODE	**HSE-P4**
NAME	**Security, privacy, and protection of clients' health information are core needs of Uganda's health system**
STATEMENT	Security, privacy, and protection of clients' health information are integral to Uganda's health system's operations and are part of Digital Health innovations. Therefore, all citizens' health information should be protected against unauthorised access and intentional and accidental modifications.
RATIONALE	Protection of clients' confidential health information will increase public trust in Digital Health and improve their utilization to deliver healthcare services
IMPLICATION	• The business context should define security and privacy requirements to be integrated into the entire Digital Health ecosystem • Digital Health systems should embed national policies to minimise improper data use and security violations • Apply security and privacy information management policies and monitor compliance • Information security controls should be clearly defined to balance cost and mitigate risks

Component 3B: MoH Digital Health Architecture Principles

Architecture principles are a set of principles that relate to architectural work. They reflect consensus across the enterprise and embody the spirit of Enterprise Architecture. Architecture Principles govern the architecture process, affecting the Enterprise Architecture's development, maintenance, and use (Josey et al., 2018). This section provides the Digital Health architecture principles for Uganda's health system. These principles shall support the health sector in delivering Digital Health solutions that are interoperable, flexible, and fit-for-purpose while supporting established guidelines, policies, and processes

for communication and use of information within Uganda's health system. They are not only expected to act as drivers for defining functional requirements for the architecture but will also be used as a guide when assessing Digital Health innovations.

The Digital Health Architecture principles listed in **Table 3 – Table 8** are categorised under four architecture domains: business, data, application, and technology. They comprise five *Business architecture (B) principles*, six *data architecture (D) principles*, three *application architecture (A) principles*, and two *technology architecture (T) principles*, *five Security and Privacy Principles (SP)*, *and two Interoperability (I) principles* as discussed in the subsequent sub-sections. Each principle has a code, statement, rationale, and implication. The principal code (code) represents the type or category of principle (i.e., *Business architecture (B)*, data *architecture (D)*, *application architecture (A)* and *technology architecture (T)*, *Interoperability (I)*, *Security and Privacy (S)*, and the principle number (e.g., P1).

Table 3. MoH Business Architecture Principles

CODE	**B-P1**
NAME	**Adhere to the Architecture Principles**
STATEMENT	The architectural principles defined apply to all Health organisations within Uganda's healthcare systems
RATIONALE	• The effectiveness of a Digital Health Architecture in providing a consistent and measurable level of quality information to decision-makers depends upon all Health organisations abiding by the principles upon which that architecture was designed • Without this principle, inconsistency, exclusion, and favoritism would rapidly undermine the information management required to achieve Uganda's health sector's strategic direction • These principles shall guide the selection, creation, and implementation of Digital Health and provide a workable transition path to targeted architecture, maintain flexibility and enhance interoperability
IMPLICATION	• All Digital Health architecture developments and new solutions should align with the principles • Digital Health solution owners and or leads should ensure that solutions comply with the principles
CODE	**B-P2**
NAME	**Engage with all relevant Digital Health stakeholders**
STATEMENT	Developers of Digital Health architecture designs, standards, and solution must collaborate with all stakeholders
RATIONALE	The Digital Health ecosystem for Uganda involves a diverse and vast community of stakeholders. Therefore, an inclusive and participatory development approach is required to address the collective set of stakeholder requirements. Using a participatory approach provides the most significant probability of achieving a successful and acceptable Digital Health solution outcome.
IMPLICATION	• Digital Health stakeholders within a community should be allowed to express their opinions when submitting requirements and providing feedback to developers and implementers • Sustained, ongoing engagement will be required to ensure collective appreciation and buy-in of architectural decisions
CODE	**B-P3**

NAME	**Ensure Digital Health solutions are fit-for-purpose**
STATEMENT	All Digital Health architecture decisions should consider the business constraints and requirements of the healthcare community
RATIONALE	• The adoption and uptake of Digital Health is dependent on: a) how well implementers of Digital Health have practically implemented and integrated it into current healthcare community practices b) the extent to which these result into overall healthcare outcomes and process improvement
IMPLICATION	• Digital Health Implementing Partners must support requirements management at all stages of architecture development, standards specifications, system implementation, system operations, and change management • Benefits realised from all Digital Health interventions must be measurable • Implementers should consider the usability of Digital Health systems when designing Digital Health solutions interventions
CODE	**B-P4**
NAME	**Support services-based approaches**
STATEMENT	Implementers must apply a service-oriented approach when developing Digital Health solutions
RATIONALE	• Service orientation delivers agility • Business services are the fundamental mechanism for sharing information and are essential building blocks for building interoperable Digital Health systems. One or more application services can support a business service.
IMPLICATION	• Identify standard services that the other systems can re-use • Business services identify information artefacts associated with service provision and use. Therefore, information models must be related to business services to determine the benefit to the health organisation.
CODE	**B-P5**
NAME	**Assess the Total Cost of Ownership of Digital Health solutions**
STATEMENT	The deployment of a new Digital Health capability should be based on an assessment of its business and social value as well as the implementation and operational costs
RATIONALE	New Digital Health capabilities are expected to support better healthcare; however, this would involve both technology and organisational change costs. Therefore, the operational cost of a solution must be identified and contained to ensure that the ongoing operation of the solution is feasible and viable.
IMPLICATION	• When making decisions to create a new Digital Health capability, stakeholders must consider the total cost of developing and maintaining the Digital Health solution • Digital Health solutions should be acquired or developed, deployed, replaced and decommissioned at the least cost while ensuring fitness for purpose of an overall system • Operational procedures and their likely cost must be identified early in selecting and developing a Digital Health solution • The deployment, migration, and cutover strategy for any Digital Health solution must be identified in assessing operational costs
CODE	**B-P6**
NAME	**Ensure Supportability, Sustainability, and Continuity**
STATEMENT	Digital Health solutions should be supportable, sustainable, and should be able to provide the required degree of business continuity necessary for their operations

RATIONALE	• The reliability of the Digital Health solutions must be considered throughout their design and use. If a Digital Health solution is to be adopted and embraced, it needs to be readily supportable, sustainable, and provide a business continuity of operation exceeding routine expectations • Users must be provided with the capability to continue business operations regardless of the failure of a Digital Health solutions • Hardware/software failure and data corruption should not be allowed to disrupt the delivery of healthcare and services
IMPLICATION	• Dependency on Digital Health mandates that the risks of healthcare delivery interruption must be established in advance and managed. Periodic reviews of the Digital Health solutions should be carried out to assure healthcare continuity. • Recoverability, redundancy, and maintainability should be addressed at the design time. • All Digital Health solutions that are critical in healthcare delivery must be assessed to determine what level of continuity is required and the necessary recovery plan.
CODE	**B-P7**
NAME	**Support use of Enterprise-wide Digital Health Solutions**
STATEMENT	The development of Digital Health solutions that are usable across Uganda's health ecosystem is preferred over the development of similar or duplicative applications which support a single Health organisation or disease domain
RATIONALE	Duplicative capability is expensive and proliferates conflicting data
IMPLICATION	• Health organisations which depend on a Digital Health solution that do not serve the entire health continuum must change over to health sector-wide solutions. This will require the establishment of an adherence policy. • Health organisations shall not be allowed to develop Digital Health solutions that are similar/duplicative to health sector-wide solutions. In this way, expenditures of resources to build duplicate Digital Health solutions will be reduced.
CODE	**B-P8**
NAME	**Comply with Laws, Policies, and Regulations**
STATEMENT	Digital Health solutions and infrastructure should comply with applicable legislation and policies in all jurisdictions and organisations within which they operate
RATIONALE	• Digital Health systems should comply with all applicable legislation, regulation, and standards. Compliance is key to maintaining stakeholder trust (Quality assurance) in the services that Digital Health solutions provide.
IMPLICATION	• Define applicable legislative and policy requirements for all Digital Health solutions and infrastructure; otherwise, there is a risk of non-compliance. These requirements should be kept up to date to reflect changes in legislation and policy • Digital Health developers and implementers must be compliant with laws, regulations, and external policies regarding the collection, retention, management and dissemination of health data • Particular attention needs to be given to Uganda's Data Protection and Privacy Act 2019 and the Data Protection and Privacy Regulations, 2020 and which regulate how organisations collect, use, disclose and secure personal information and provide individuals with rights of access and correction. All health service providers must comply with the Data Protection and Privacy Act and any other laws that relate to data security including the National Information Security Policy. The National Information Policy outlines the minimum-security controls that all public and private organisation must meet • Rather than prescribing implementation mechanisms, policy requirements should be expressed in terms of obligations, permissions, prohibitions, outcomes, and performance requirements

Table 4. MoH Data Architecture Principles

CODE	**D-P1**
NAME	**Manage Health Data as an Asset**
STATEMENT	Health data must be managed so that its source and the times and places it is created, changed, updated, accessed, and ultimately disposed of are captured and retained.
RATIONALE	Health data is the foundation of decision-making within healthcare, so it must be carefully managed to ensure that we know where it is, rely upon its accuracy, and obtain it when and where we need it. Effective health data management ensures evidence-based decision-making & improved healthcare outcomes. Organizing and managing the critical data assets drives the business processes required to support healthcare service delivery.
IMPLICATION	• Health data components should always identify the time and place of information creation and change. Versioning and metadata are one way of capturing this. • Services providing sharing or access to information may keep only the most recent or most accurate version but must acknowledge the existence of preceding versions. • Uganda's health system must have a cultural transformation from "data ownership" thinking to "data stewardship" thinking. • Data stewards must have the authority and means to manage the data they are accountable for. Part of the role of the data steward is to ensure data quality. • Procedures must be developed and used to prevent and correct errors in Digital Health solutions. • Steps to ensure the quality of data held by the Digital Health solutions should be implemented.
CODE	**D-P2**
NAME	**Ensure Data Consistency in Distributed Environments**
STATEMENT	A distributed Digital Health environment requires explicit support for ensuring consistency and completeness of data originating from multiple sources.
RATIONALE	Digital Health components and services typically span organisational and geographic boundaries affecting the reliability, availability, and performance of data processing. Atomic transactions cannot generally address the scalability, autonomy, and robustness issues in such an environment, so a process-centric approach to consistency must be adopted. This is particularly important for sporadically connected systems and long-running transactions or processes.
IMPLICATION	• The process for establishing consistency of information should be explicitly defined for service usage scenarios. • Atomic transaction mechanisms may be used across services, but an alternate mechanism should always be provided to achieve consistency through discrete steps when information crosses organisational boundaries. • When developing processes, the needs of sporadically connected participants must be considered to ensure consistency. • Transactional messaging is a valuable and robust mechanism that can support consistency processes but is not generally sufficient; a consistency process definition is still required. • The time and place attributes of an information component (see D.P1) can be used to help establish consistency.
CODE	**D-P3**
NAME	**Ensure Data Sharing across Uganda's Health System**

STATEMENT	Data held by Digital Health solutions should be shareable across Health organisations. Users of Digital Health should have access to the necessary shared data required to perform their respective business functions. In addition, shared data should be centrally controlled and managed.
RATIONALE	· Electronically shared data will increase efficiency as Health organisations can use it, without rekeying, to create new entities. · Users will rely on official sources of more accurate and timely managed data, thereby improving decision-making.
IMPLICATION	A common set of standards, policies, and procedures that users should adhere to should be developed to enable data sharing among Health organisations. • Standard data models, data elements, and other metadata that define the shared environment should be developed and stored in a repository for easy access. • This principle of data sharing held by Digital Health solutions will continually "bump up against" the principle of data security. However, under no circumstances will the data sharing principle result in confidential data held by the Digital Health systems being compromised. • All users will have to rely on electronic data made available for sharing to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision-making.
CODE	**D-P4**
NAME	**Ensure Data Ownership and Responsibility**
STATEMENT	• Health organisations must own each data entity held by Digital Health systems. Every Health organisation should be responsible for the integrity and security of its data. Therefore, each data entity held by Digital Health systems must have an owner. • *Primary Data Source*: All health data should have an authoritative, official, primary data source, which should be the location for all "create", "update" and "delete" actions but this should be in line with data management guidelines of the health sector.
RATIONALE	• The lack of a well-defined data ownership may lead to confusion about who can change the data held by the Digital Health systems. Identifying the Health organisation's ownership of its respective data entities avoids ambiguity and creates clear responsibility and accountability for all data. • Identifying the data owners will clearly define the point of contact in the respective unit responsible and accountable for all changes in the data entities held by the Digital Health systems. • For data to be managed effectively, there can be only one primary source for each data entity. This will enable a data entity to be traceable back to the source. Otherwise, inconsistent, erroneous, and out-of-date data may result. • Data integrity is at its highest level when data changes are centrally done.
IMPLICATION	• The data owner shall be responsible for meeting quality requirements levied upon the data. • Health data shall be captured once and immediately validated at the source. In addition, quality control measures must be implemented to ensure the integrity of the data.
CODE	**D-P5**
NAME	**Use Common Terminologies and Data Definitions**
STATEMENT	• There should be a standard, common and consistent definition of all data held by the Digital Health systems, which should be understandable and available to all users. • Data held by the Digital Health systems should be defined to ensure seamless interoperability.
RATIONALE	• Electronic data to be exchanged across the health sector and should have a standard definition with an agreed format and meaning of the data items. A common vocabulary facilitates effective communications and enables sharing of data. • Electronic data sharing also enhances metadata modeling, consistency, and quality

	• Centralized metadata provides a single point for maintaining the metadata.
IMPLICATION	• Common terminologies for the services must be established. The definitions shall be used uniformly throughout the Digital Health solutions. • Ambiguities resulting from multiple parochial definitions of data must give way to accepted health sector-wide definitions and understanding • The MoH shall coordinate all the data standardisation initiatives

Table 5. MoH Application Architecture Principles

CODE	**A-P1**
NAME	**Promote the development of modular and component-based Digital Health solutions**
STATEMENT	• Digital Health solutions should be modular and component-based, aligned to business processes. • They should also conform to established open standards with well-defined roles & responsibilities. • Components should be independent of the physical topology of the system and scalable.
RATIONALE	Reduces total cost of ownership and avoids vendor lock-in
IMPLICATION	· Avoid proprietary solutions and technologies if possible. · Consider use of the latest web services, XML and integration standards in line with GoU eGovernment Web applications security (WASA) framework. · Internet-based web standards and technology should be preferred for all solutions.
CODE	**A-P2**
NAME	**Ensure ease of use of solution**
STATEMENT	Digital Health solutions should be easy to use. Developers of Digital Health solutions must ensure that the underlying technology is transparent to users. This will allow users to concentrate on the tasks at hand.
RATIONALE	• The more a user has to understand the underlying technology, the less productive that user is. Ease of use is a positive incentive for the use of a Digital Health system. • It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish tasks. Training shall be kept to a minimum, and the risk of misusing a Digital Health solution will reduce.
IMPLICATION	• Digital Health applications shall be required to have a common "look and feel." Hence, the common look and feel standard must be designed, and usability test criteria must be developed. • Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. Instead, factors such as linguistics, customer physical infirmities (visual acuity, ability to use keyboard/mouse), and proficiency in using technology have broad ramifications in determining the ease of use of an application. • The Digital Health solutions should define and communicate the right of access and use.
CODE	**A-P3**
NAME	**Ensure technology independence of solutions**
STATEMENT	Digital Health solutions should be independent of specific technology choices. They should be able to operate on a variety of technology platforms.

RATIONALE	Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way.
IMPLICATION	• Developers should adopt standards that support portability while developing Digital Health solutions. • Subsystem interfaces should be developed to enable existing systems to interoperate with the new Digital Health system. • Developers are encouraged to use programming software, which give a high degree of priority to platform-independence.

Table 6. Digital Health Technology Architecture Principles

CODE	**T-P1**
NAME	**Embrace Requirements-Based Change**
STATEMENT	Changes to Digital Health technology infrastructure should be made in response to the business needs of the health organisation.
RATIONALE	This principle will foster an atmosphere where the Digital Health technology infrastructure changes in response to the business needs and requirements of the health organisations, rather than having it change in response to IT changes. This shall ensure that business drives changes to Digital Health. Unintended effects on business due to IT changes will be minimised. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.
IMPLICATION	• Changes to Digital Health technology infrastructure shall follow a complete examination of the proposed changes using the Digital Health Enterprise Architecture. • The need for financial and technical assistance should be communicated by the business need or requirement. • Change management processes conforming to this principle should be developed and implemented.
CODE	**T-P2**
NAME	**Control Technical Diversity**
STATEMENT	Technological diversity should be controlled to minimise the non-trivial cost of maintaining expertise and connectivity between multiple processing environments.
RATIONALE	There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. More infrastructure costs are incurred to keep multiple processor constructs interconnected and maintained. Limiting the number of supported components will simplify maintainability and reduce costs.
IMPLICATION	• Policies, standards, and procedures that govern the acquisition of technology must be tied directly to this principle. • Technology choices for Digital Health solutions shall be constrained by the options available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and embraced. • The technology blueprint of Digital Health shall only change when compatibility with current infrastructure improvement in operational efficiency or a required capability has been demonstrated.

Table 7. MoH Interoperability Principles

CODE	**I-P1**
NAME	**Re-use Digital Health components**
STATEMENT	Components and services that are re-usable across the health sector are preferred over proprietary solutions.
RATIONALE	Duplicating capability is expensive and undermines interoperability by proliferating inconsistency and ambiguity.
IMPLICATION	Where infrastructure components are provided for re-use within Digital Health solutions, adoption, integration, and use of these components should be preferred to duplicating their functionality through bespoke development.
CODE	**I-P2**
NAME	**Observe open standards**
STATEMENT	Promote adherence to open standards.
RATIONALE	• Adherence to open standards that will enhance interoperability of Digital Health. • The attributes of open standards such as platform independence, vendor neutrality, and ability to use across multiple implementations and the model for establishing open standards are what will allow for sustainable information exchange, interoperability, flexibility, data preservation & and greater freedom from technology and vendor lock-in • Adoption of open standards will facilitate storing of electronic health data using open data file formats.
IMPLICATION	• Choices should comply with the World Trade Organisation (WTO) Code of Good Practice for the adoption and application of Standards. In particular, locally contextualised standards should be used where they exist.

Table 8. MoH Security and Privacy Principles

CODE	**SP-P1**
NAME	**Align security and privacy controls to the existing legal and regulatory framework**
STATEMENT	• Security and privacy controls should be compliant with Uganda's Data Protection and Privacy Act 2019 and Data Protection and Privacy Regulations, 2020 • The selection of security controls should be based on risk analysis and risk management decisions. The process for selecting new controls should consider both the degree of risk mitigation provided by the control and the total cost to acquire, implement and maintain the control. • The selection of controls should be driven by the ability of the control to be applied uniformly across the entire health sector and to minimise exceptions.
RATIONALE	• Achieving a standards-based Digital Health security environment will reduce operational costs, improve interoperability and improve supportability.
IMPLICATION	• Health organisations should ensure that Security and privacy policies align with Uganda's National Information Security Framework.
CODE	**SP-P3**

NAME	**Incorporate Security into Architecture Design**
STATEMENT	Architectures should employ security measures to ensure integrity, confidentiality, and availability of IT services and applications. Security should be designed into the architecture in a scalable and efficient manner. The security architecture design should follow a modular design where the overall technology infrastructure is divided into functional layers/modules.
RATIONALE	The layered/modular approach allows the architecture to address the security relationship between the various functional blocks of the infrastructure. In addition, it permits designers to evaluate and implement security on a module-by-module basis instead of attempting to complete the architecture in a single phase.
IMPLICATIONS	Comprehensive published security standards for each layer/module of the IT architecture are a prerequisite for all security designs.
CODE	**SP-P4**
NAME	**Implement Least Privilege Standard**
STATEMENT	Each Digital Health solution must incorporate a standard for least privilege; thus, the baseline is the bare minimum privileges necessary to perform functions, actions, and access.
RATIONALE	The baseline for functions, actions, and access is the minimum required to complete the task, thus protecting users and the data they are using from inadvertent errors, exploitation, or attempts at deliberate misuse. Adhering to the principle of least privilege reduces the risk of attackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.
IMPLICATION	• Part of the solution design should ensure the principle of least privilege is incorporated into the solution to enhance the protection of data and functionality from faults and malicious behavior. • Contains compromises to their area of origin, stopping them from spreading. • The scope of audits can be reduced dramatically, thus ensuring the efficient use of scarce resources. • Users, clients, businesses, and the enterprise are better protected.
CODE	**SP-P5**
NAME	**Implement appropriate Privacy and Security Safeguards**
STATEMENT	Appropriate technical and organisational controls must be implemented to protect data and keep it confidential.
RATIONALE	The privacy and security of data are everyone's responsibility. The Data Protection and Privacy Act 2020 requires organisations that process personal data to ensure they maintain the security and privacy of this data. It is necessary to have policies and security safeguards implemented to protect health information, whether stored on paper or electronically.
IMPLICATIONS	• Access controls – Access to information should be on a need-to-know basis, with role-based access. • Technical controls – Implement robust IT security controls such as password authentication, encryption, anti-malware software, patch management, firewalls, IDS, mobile device management, secure code reviews, etc. • Auditing – Digital Health systems should be audited at least twice a year. • Incident detection & response – continuous monitoring to identify and respond to threats.

COMPONENT 4: ARCHITECTURE PROCESS

The DHEAF includes an architecture process illustrated in **Figure 5** that addresses the Enterprise Architecture goals of the Digital Health initiatives. The cycle is enclosed by the architecture catalysts previously introduced so that all activities, deliverables, and guidelines are aligned to the constituents for the EA development to deliver a successful digital transformation initiative. The DHEAF development process is based on the TOGAF Architecture Development Model (ADM) cycle and impersonates the architecture development structure of TOGAF. The TOGAF ADM is a generic and reliable method for architecture development, designed to deal with most systems and organisational requirements (The Open Group, 2018a).

The architecture process provides for the development and implementation of Enterprise Architectures that address the goals and objectives of the health organisations. The architecture process phases include business, application, data, and technology, followed by opportunities and solutions, migration planning, implementation governance, and change management that work in conjunction with procedures laid down in the eHealth Policy framework for Uganda. In addition, the Architecture Process emphasises requirements management at every stage and includes governance via several governance bodies highlighted in the EA governance model. It is, however, important to note that in navigating the architecture process, architects should leverage the re-usable assets that are part of this framework. These assets include; reference models for Business, Data, Application, Technology, and services, Information security architecture, and Health Information Exchange (HIE) model. Others include; the Digital Health capability model, Interoperability standards, Monitoring and Evaluation model, and the DH capacity building/skills model. **Figure 5** illustrates the phases of the architecture process for Digital Health including the respective phase associated activities and expected architecture inputs and outputs. It is also necessary that the requirements are identified, stored, and input into all activities in the architecture process. Health organisations should define all the non-functional requirements of the solution they would like to implement. The architecture team should consider the domain-specific principles that derive the requirements and existing Digital Health Policies and standards when defining requirements.

Description of the phases in the Architecture process

Preliminary Phase

The Preliminary Phase prepares a health organisation for a successful EA project. It mainly focuses on the preparation and initiation activities required to meet a business directive for digital transformation. Specifically, it is concerned with determining and establishing the architecture capability needed by a health organisation and defining the principles that will constrain the digital transformation effort. Activities involved in this phase include; scoping the health organisation's units to be impacted by the digital transformation effort, establishing architecture principles, and developing a strategy and implementation plan for the productivity tools (i.e., Modelling) that will be required. **Table 9** outlines the critical inputs and outputs of the preliminary phase.

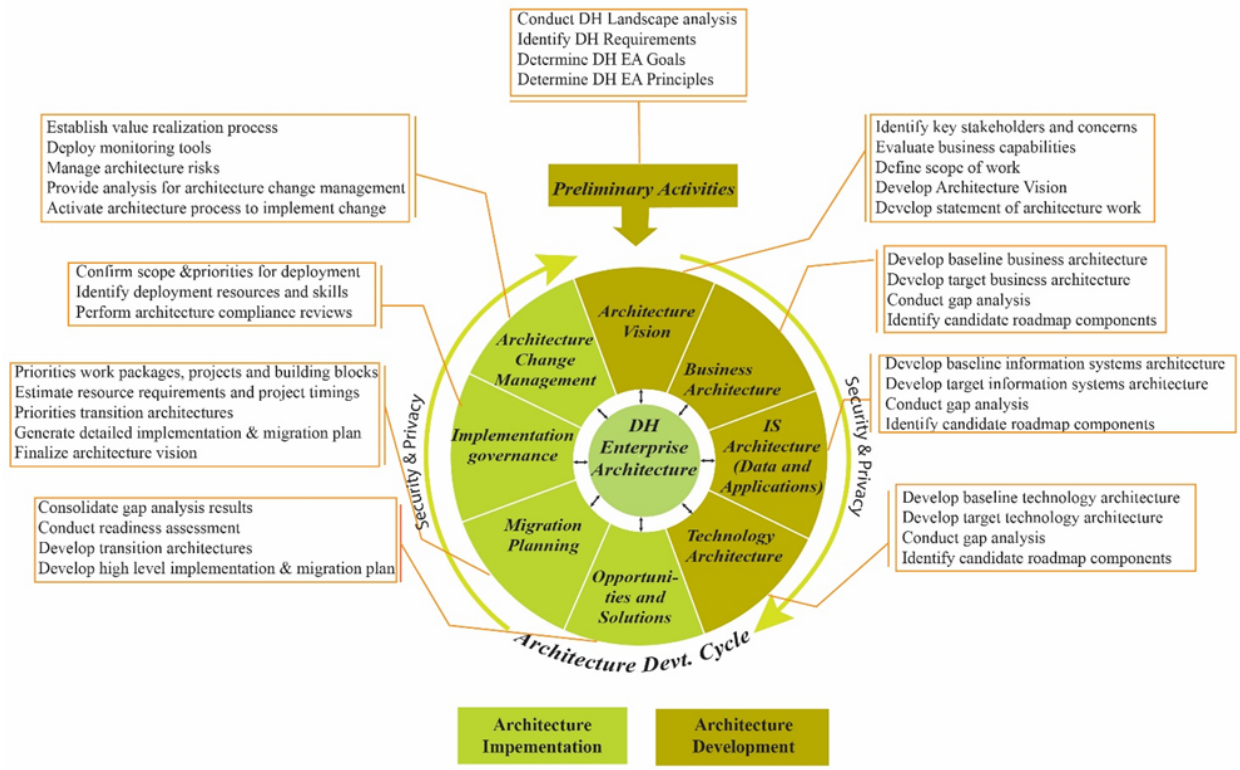


Figure 5. Architecture Process (Adopted from The Open Group,2018)

Table 9. Inputs and Outputs of Preliminary Phase

Inputs	• Business strategies, business goals, and business principles of the health organisation • Governance and legal frameworks relevant to Digital Health • Partnerships and Contracts agreements • National eHealth Strategy for Uganda
Outputs	• Organisational Model for Enterprise Architecture specifying the units that will be part of the initiative • Request for Architecture Work

Architecture Vision

The Architecture Vision phase defines the scope of the architecture effort and the constraints that the health organisation must deal with. The primary goal of this phase is to create a high-level aspirational vision of the business capabilities targeted by the health organisation. Therefore, critical activities of this phase should include; identifying key stakeholders and their concerns, evaluating business capabilities, defining the scope of work, and developing an Architecture Vision. Furthermore, when documenting the Architecture Vision, architects need to show the value proposition for each category of stakeholders in the digital transformation effort. Also, as part of this phase, the architects must go through all the formal processes of seeking approval of the Statement of Architecture Work Approved by the relevant authorities. **Table 10** shows key inputs and outputs of the Architecture Vision phase.

Table 10. Inputs and Outputs of Architecture Vision Phase

Inputs	• Organisational Model for Enterprise Architecture specifying the units that will be part of the initiative • Request for Architecture Work
Outputs	• Approved statement of Architecture Work • Capability assessments • Architecture Vision including high-level stakeholder requirements • Draft Architecture definition document including; o Baseline Business, Data, Application, and Technology Architecture (high-level)

Business Architecture

This phase elaborates a Business Architecture based on the agreed-upon Architecture Vision. Specifically, it identifies business capabilities and processes, services, and actors in the current state and those required in the future. The principal technique applied here is Business Capability Modelling (BCM), used with business process models. All process models should be associated with enterprise-level information entities to reflect what business objects are accessed or realised as they are executed. Activities of the Business Architecture phase include; developing the baseline and target business architecture describing the product/service strategy, organisation structure, functional processes, business goals, etc. Other activities include analysing the gaps between baseline and target business architectures and identifying business architecture's candidate road map components. **Table 11** shows key inputs and outputs of the Business Architecture phase.

Table 11. Inputs and Outputs of Business Architecture Phase

Inputs	• Approved Statement of Architecture Work
	• Capability Assessments
	• Business principles, business goals, business drivers
	• Architecture Vision including key refined high-level stakeholder requirements
	• Draft Architecture definition document including;
	  o Baseline Business, Data, Application, and Technology Architectures (high-level)
	  o Target Business, Data, Application, and Technology Architectures (high-level)

Outputs	• Draft Architecture Definition Document containing content updates:
	  o Baseline Business Architecture (detailed), if appropriate
	  o Target Business Architecture (detailed with Business Capabilities, business processes, and Organisation Map as core artefacts)
	• Draft Architecture Requirements Specification document including content updates:
	  o Gap analysis results
	  o Technical requirements
	• Updated business requirements
	• Business Architecture components of an Architecture Roadmap

Information Systems Architecture

The Information Security Architecture Phase is concerned with identifying and defining the *applications* and *data* considerations that support a health organisation's business architecture

developed in the previous phase. In this phase, the architects create both the Data and Application Architecture, which they may design either sequentially or concurrently.

Data Architecture

Data Architecture Phase is concerned with defining the data considerations that support the Business Architecture, including; data management (i.e., collection, processing, storage, and dissemination), migration, and governance. As part of the Data Architecture, the architecture team should consider developing the Application/Organisation, Role/Application, Application Interaction, and Application Function matrices. These matrices enable the architecture team to identify user and organisational dependencies on applications. In addition, this will support future state planning by determining impacted user communities and facilitating application grouping by user type or user location. **Table 12** shows the key inputs and outputs of the Data Architecture phase.

Table 12. Inputs and Outputs of Data Architecture Phase

Inputs	• Approved Statement of Architecture Work
	• Capability Assessments
	• Data principles
	• Architecture Vision
	• Draft Architecture definition document including;
	  ○ Baseline Business, Data, Application, and Technology Architectures (high-level)
	  ○ Target Business, Data, Application, and Technology Architectures (high-level)

Outputs	• Draft Architecture Definition Document containing content updates:
	  ○ Baseline Data Architecture (detailed), if appropriate
	  ○ Target Data Architecture (detailed).
	• Draft Architecture Requirements Specification document including content updates:
	  ○ Gap analysis results
	  ○ Data interoperability requirements
	• Relevant technical requirements that will apply to the digital transformation effort
	• Constraints in the Technology Architecture
	• Data Architecture components of an Architecture Roadmap

Applications Architecture

This phase is concerned with defining the application components and or subsystems required to support the business architecture, including; services, major functions, and interfaces. It shows how the application layer components map onto the Business Architecture. However, it is important to note that this phase is not concerned with application system design but is concerned with defining what kind of systems are relevant to Uganda's health sector. As part of this phase, the architecture team is encouraged to take advantage of relevant Application Architecture resources provided by:

- The TOGAF Integrated Information Infrastructure Reference Model (III-RM) — focuses on the application-level components and services necessary to provide an integrated information infrastructure ((The Open Group, 2018b))
- The Object Management Group (OMG) — has several software models relevant to domains such as healthcare (www.omg.org)

Key activities of the Application Architecture Phase should include developing the baseline and target Application Architectures, gap analysis, and identification of Application Architecture components of the Architecture Roadmap. **Table 13** shows the key inputs and outputs of the Application Architecture phase.

Table 13. Inputs and Outputs of Application Architecture Phase

Inputs	• Approved Statement of Architecture Work
	• Capability Assessments
	• Application principles
	• Architecture Vision
	• Draft Architecture definition document including;
	  o Baseline Business, Data, Application, and Technology Architectures (high-level)
	  o Target Business, Data, Application, and Technology Architectures (high-level)

Outputs	• Draft Architecture Definition Document containing content updates:
	  o Baseline Application Architecture (detailed), if appropriate
	  o Target Application Architecture (detailed)
	• Draft Architecture Requirements Specification document including content updates:
	  o Gap analysis results
	  o Application interoperability requirements
	  o Relevant technical requirements that will apply to the digital transformation effort
	• Constraints in the Technology Architecture
	• Data Architecture components of an Architecture Roadmap

Technology Architecture

The technology architecture phase maps application components defined in the Application Architecture phase into a set of technology components representing software, hardware, and communication technology. These include; computing platforms, storage, networks, operating system, middleware, database systems, other system software, and deployable artefacts. As part of this phase, the architects define new technology components introduced in the digital transformation effort. Likewise, existing technology components to be supported in the target environment may need to be re-defined to ensure fit-for-purpose and interoperability. The architecture team is encouraged to take advantage of relevant Technology Architecture resources provided to the TOGAF Technical Reference Model (TRM). Key activities for this phase should include developing baseline and target Technology Architectures, gap analysis, and identification of Technology Architecture components of the Architecture Roadmap. **Table 14** shows the key inputs and outputs of the Technology Architecture phase.

Table 14. Inputs and Outputs of Technology phase

Inputs	• Approved Statement of Architecture Work
	• Capability Assessments
	• Technology principles
	• Architecture Vision
	• Draft Architecture definition document including;
	  o Baseline Business, Data, Application, and Technology Architectures (Detailed)
	  o Target Business, Data, Application, and Technology Architectures (Detailed)

Outputs	• Draft Architecture Definition Document containing content updates: o Baseline Technology Architecture (detailed), if appropriate o Target Technology Architecture (detailed) • Draft Architecture Requirements Specification document including content updates: o Gap analysis results o Technology interoperability requirements o Relevant technical requirements that will apply to the digital transformation effort • Constraints in the Technology Architecture • Technology Architecture components of an Architecture Roadmap

Opportunities and Solutions

This phase is concerned with identifying delivery vehicles (projects, programs, or portfolios) that will successfully deliver the Target Architecture identified in the business, application, and technology architecture phases. As part of this phase, the architecture team should review the target business objectives and capabilities of the health organisation, consolidate the gap analysis results and the interoperability requirements from the Business to Technology Architecture phase, and then organize groups of building blocks to address these capabilities. The architecture team should also conduct readiness assessment exercises to evaluate the health organisation's ability to absorb change. Finally, centering on the readiness assessment results, the architecture team should develop a series of Transition Architectures (delivery vehicles) to generate a high-level Implementation and Migration plan. **Table 15** shows the key inputs and outputs of the Opportunities and Solutions phase.

Table 15. Inputs and Outputs of Technology phase

Inputs	• Capability Assessments • Enterprise Architecture Governance Model/framework • Statement of Architecture Work • Architecture Vision • Draft Architecture Definition Document • Draft Architecture Requirements Specification Document • Change requests from existing Digital Health Programs/Projects • Candidate roadmap components from Business, Information system, and Technology Phases.
Outputs	• Capability Assessments including; o Business Capability o IT Capability • Architecture Roadmap including; o Identified Transition Architecture o Work package portfolio o Implementation recommendations • High-level Implementation and Migration Plan including; o Implementation and Migration Strategy

Migration Planning

Migration planning is concerned with formulating a detailed Implementation and Migration Plan that will realise some or all of the Transition Architectures identified in the opportunities and solution phase. **Table 16** shows the inputs and outputs of the migration planning phase. phase Key activities of this phase should include:

- Coordinating the implementation and migration plan with the various management frameworks within the health organisation, including project planning and business planning. Enterprise Architecture and operations management.
- Prioritising all work packages, projects, and building blocks by assigning business value to each and conducting a cost/business analysis. Business value must be associated with the capabilities at this stage, and capability increments should be used to assign the business values.
- Estimating resource requirements, project timings, and availability/delivery vehicles. When estimating resource requirements, costs should be divided into capital (to create the capability) and operations and maintenance (to run and sustain the capability).
- Prioritising the transition architectures/delivery vehicle through conducting a cost/benefit assessment and Risk authentication.
- Generating a completed Implementation and Migration Plan. This should include integrating all project activities, dependencies, and the impact of change into a project plan.
- Finalising the Architecture Vision and Architecture Definition Documents, in line with the agreed implementation approach.

Table 16. Inputs and Outputs of the migration planning phase

Inputs	• Capability Assessments • Statement of Architecture Work • Architecture Vision • Draft Architecture Definition Document • Draft Architecture Requirements Specification Document • Change requests from existing Digital Health Programs/Projects • Architecture Roadmap • High-level Implementation and Migration Plan
Outputs	• Implementation and Migration Plan (detailed), including: o Implementation and Migration Strategy o Project and portfolio breakdown of the implementation • Finalised Architecture Requirements Specification • Finalised Architecture Roadmap Re-usable

Implementation Governance

This phase is concerned with providing an architectural oversight of implementing the target Digital Health architecture for Health organisations. Key activities of this phase include;

- Confirming scope and priorities for deployment with development management. The implementation team should review the migration planning outputs and produce recommendations for deployment. It should also identify building blocks for replacement, perform a gap analysis between the DH Architecture and solutions framework and produce a gap analysis report to guide implementation decisions.

- Identifying deployment resources and skills required for the deployment team. Additionally, the deployment team should be educated about the overall architecture deliverables and expectations from specific development and implementation projects.
- Performing architecture compliance reviews for each transition architecture. The compliance review must follow the compliance review process in the Enterprise Architecture Governance model. **Table 17** shows the inputs and outputs of the Implementation governance phase.

Table 17. Inputs and Outputs of Implementation Governance

Inputs	• Capability Assessment • Statement of Architecture Work • Architecture Vision • Architecture Definition Document • Architecture Requirements Specification • Architecture Roadmap • Digital Health Enterprise Architecture Governance Model • Implementation and Migration Plan (Detailed)
Outputs	• Compliance Assessments • Change requests • Deployed Architecture compliant Digital Health solutions, including; o Architecture-compliant implemented system o Populated Architecture Repository o Architecture compliance recommendations and dispensations o Recommendations on service delivery requirements o Recommendations on performance metrics o Service Level Agreements (SLAs) o Architecture Vision, updated post-implementation o Architecture Definition Document, updated post-implementation

Architecture Change Management

The Architecture Change Management phase establishes procedures for managing change to the new Digital Health architecture. The goal is to ensure that the architecture achieves its original target business value. Part of this phase requires the architecture team to continuously monitor governance requests, developments in technology, and changes in the business environment. In addition, the architecture team should put in place a change management process for the implemented architecture. The change management process, once established, will help to determine:

- Circumstances under which the implemented architecture, or parts of it, will be permitted to change and the process by which that will happen;
- The circumstances under which the architecture development process will be initiated again to develop a new architecture.

Table 18 shows the inputs and outputs of the architecture change management phase. Key activities of this phase should include:

- Establishing a value realisation process. The architecture team should engage stakeholders and agree on the Key Performance Indicators (KPIs) for each transition architecture/delivery vehicle.
- Deploying monitoring tools to support:
    - The business and technology changes could impact Digital Health Enterprise Architecture for the health organisation.
    - Business value tracking; e.g., investment appraisal method to determine value metrics for the business objectives.
    - Monitoring Enterprise Architecture Capability maturity of the health organisation
    - Tracking Quality of Service (QoS) performances and usage
- Managing architecture risks and providing recommendations on how the risks can be mitigated. In performing this activity, the architecture team is encouraged to use the approved Risk Management Framework for the MoH. If this is not available, the architecture team may adopt the Risk management process part in the Digital Health Enterprise Architecture Governance Model.
- Providing analysis for architecture change management, including:
    - Conducting architecture performance reviews;
    - Assessing requests for change and reporting to ensure that the expected value realisation and Service-Level Agreement (SLA) expectations are met;
    - Undertaking a gap analysis of the performance of the architecture;
    - Ensuring that requests for change adhere to the Request for Change that is part of the Digital Health Enterprise Architecture Governance Model;
    - Documenting recommendations on change requirements to meet performance targets;
- Activating the architecture process to implement the required change. This involves the development of a new Request for Architecture Work.

Table 18. Inputs and Outputs of Architecture Change Management Phase

Inputs	• Statement of Architecture Work • Architecture Vision • Architecture Definition Document • Architecture Requirements Specification • Architecture Roadmap • Request for Change due to business and technology changes • Compliance Assessments • Implementation and Migration Plan
Outputs	• Architecture updates • Changes to architecture vision and principles • New Request for Architecture Work

COMPONENT 5: DIGITAL HEALTH MONITORING & EVALUATION

Evaluation of Digital Health interventions helps to generate data that can be used as a basis for assessing whether observed changes in behavior, processes or health outcomes can be attributed to the Digital Health interventions (Lau & Kuziemsky, 2016; WHO, 2016). ***Evaluation*** is defined as a systematic and objective assessment of an intervention that aims to determine the fulfillment of objectives, efficiency, effectiveness, impact and sustainability (WHO, 2013). ***Monitoring*** is the routine collection, review, and analysis of data intended to measure implementation progress for Digital Health initiatives, and results into adjustments in intervention activities necessary to maintain or improve the quality and consistency of the Digital Health deployment.

The Digital Health Monitoring and Evaluation Framework (DHM&EF) aims to guide the process of monitoring DH implementations and evaluation of DH results in terms of outcomes and impact on healthcare in Uganda. The DHM&EF constitutes of three components; i). a *reference model* that demonstrates key aspects of DH monitoring and evaluation; ii). *performance indicators* for measuring DH performance and how these can be operationalized; and iii). a *set of guidelines* on how to conduct monitoring and evaluation of Digital Health interventions.

The Digital Health evaluation reference model (**Figure 6**) provides a basis for evaluating the performance of Digital Health implementations along the results chain (**Appendix 2**), starting with the programme inputs and activities until the impact. The model indicates the key Digital Health evaluation questions that should be answered; the key domains of performance indicators, and the data sources where the data needed to measure the indicators can be collected from at each stage of the results chain.

Monitoring of programme inputs and activities answers whether the DH technology works; and it relates to the assessment of the feasibility of the DH implementation and the inputs for developing the initiative. Monitoring of DH outputs assess how the users interact with the initiative; and it relates to the service output measures intended to capture and assess the immediate results of the DH initiative as well as the usability measures to help quantify how the users interact with it.

Evaluation of DH outcomes help to ascertain how the DH improves programme processes and service delivery; and it captures the effect of the Digital Health implementation on programme service utilization outputs or the extent to which the clients use the programme service, and intermediate population-level outcomes. The "*evaluation of impact*" focuses on establishing how improvements in service delivery impact health by capturing long-term outcomes, and impact on health that are attributed to the health intervention being supported by the DH initiative.

Digital Health Monitoring and Evaluation Reference Model

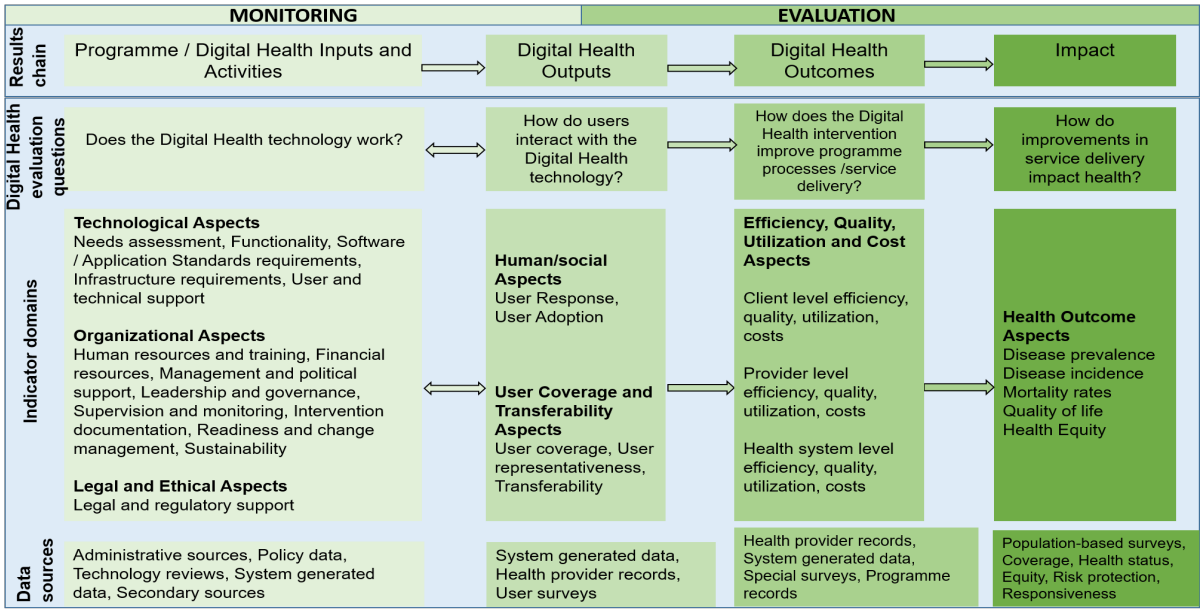


Figure 6. Digital Health Evaluation Reference Model (Adopted from Ashaba & Nabukenya, 2022)

Also, to note is a feedback loop in monitoring of the programme inputs and activities, and DH outputs. From a technical perspective, DH inputs affect the respective outputs and users' experience, while the user experience/feedback informs the DH development process. Feedback from end-user adoption and satisfaction rates loops around to further inform the DH development process and determines the quality of the technological inputs. This, in turn, affects the performance of the revised version of the DH system among end-users, making the technology development process iterative.

DHM & EF Evaluation Indicators and Operationalisation Tools

The DHM&EF Evaluation indicators and operationalisation tools (**Appendix C1**) demonstrate how the DH interventions' performance can be measured at each stage of the results chain in the reference model. To note is that, this set of example indicators and operationalisation tools are general and non-exhaustive; henceforth requiring that priority indicators and their operationalisation tools for use to monitor and evaluate a specific DH intervention should be selected based on the relevance of the intervention and modified to reflect the specific objectives of the intervention.

DH Interventions' Evaluation Guidelines

The last component of the DHM&EF Evaluation framework provides a set of guidelines (strategies and course-of-actions) that are intended to guide/facilitate the users through a step-by-step process of planning and executing activities for monitoring and evaluation of DH interventions. These should be followed with adaptation to the DH context.

1. Establish dedicated resources and effort to ensure an effective process, and such considerations should be provided from the inception of the initiative. DH implementers should plan and budget for monitoring and evaluation of the interventions during

planning and costing of their DH programmes, to ensure that appropriate resources are dedicated (WHO & ITU, 2012).

2. Identify all key stakeholders of the DH initiative, involve them and consider their interests in the DH intervention while designing the monitoring and evaluation plans, and ensure their consensus on the public health need or goal that the DH addresses or supports (WHO, 2016).
3. Make use of/refer to the DH reference model, indicator domains and sub-domains as well as the example indicators as guides to think through the necessary monitoring and evaluation aspects of the DH intervention. The reference model provides a graphical representation to aid the clarification of monitoring and evaluation scopes and identification of expected causal links between inputs and activities, outputs, outcomes and impacts for DH implementations, while the indicator domains and indicators provide a non-exhaustive list of some examples of indicators that can be measured under each stage of the results chain.
4. Define the appropriate DH initiative implementation phases and timeframes to specify and harmonize the stages of the DH maturity, timing for delivery of the defined results and frequency of measuring the results. Defining the DH initiative implementation phases helps to refine and focus on the appropriate results and indicators to be monitored or evaluated at each stage of maturity of the DH intervention. Stakeholders should agree on the stage of maturity of the DH intervention and determine the appropriate monitoring or evaluation activities to avoid embarking on premature DH results (WHO, 2016). The mapping shown in **Error! Reference source not found.** can be used to match the six stages of maturity of a DH intervention with the results chain and DH evaluation questions.

Table 19. Mapping Digital Health maturity stages with the results chain and Digital Health evaluation questions

Stages of Digital Health maturity	**Pre-prototype**	**Prototype**	**Pilot**	**Demonstration**	**Scale-up**	**Integration/ sustainability**
Results Chain Stage	Programme and Digital Health Inputs and Activities		Digital Health Outputs	Digital Health Outcomes	Digital Health Impact	
Digital Health evaluation question	Does Digital Health technology work?		How do users interact with Digital Health?	How does Digital Health improve programme processes/ service delivery?	How do improvements in service delivery impact health?	

5. Define stakeholder priorities and their projected impact of the DH intervention and outcomes required to cause the defined impact, and the respective impact and outcome measurable indicators while ensuring that interests of all identified stakeholders are addressed. Evaluation of a DH intervention can be limited to its process and early outcomes without the need to evaluate its long-term outcomes and impact if the DH is supporting a health intervention with known efficacy based on prior research.
6. Define DH outputs required leading to each defined DH outcome and the respective DH output indicators (MoH-Uganda, 2016). The outputs should include immediate results of

the DH intervention and should also capture usability measures that help to quantify how users interact with the DH intervention.

7. Define DH inputs and activities and their respective measurable indicators while taking into consideration of all the technical, organisational, policy and behavioral factors that influence delivery of a working DH application. Indicators for availability of resources required to support monitoring and evaluation functions should also be considered while defining indicators for the DH inputs and activities.
8. Define the baseline and target measures for defined indicators to clearly label the situation before the DH implementation (baseline measures) and expected achievements (target measures) after the DH implementation (MoH-Uganda, 2016). A measure of the baseline situation facilitates the ability to compare situation statuses before and after the DH implementation. It necessitates research and analysis to determine baseline measures for each indicator, while internal analysis and input from the subject-matter experts and other health experts are necessary to determine target measures (WHO & ITU, 2012).
9. Define the necessary monitoring and evaluation governance and processes/activities (MoH-Uganda, 2016; WHO & ITU, 2012). Considering that monitoring and evaluation tasks are conducted at different and various times and by various parties, it is imperative that their governance model is defined to guide on the available functions, roles, responsibilities, and required mechanisms to deliver them.
10. Prepare for and initiate the monitoring and evaluation process that should continue ongoing in parallel with the DH implementation (MoH-Uganda, 2016; WHO & ITU, 2012) , with monitoring or evaluation undertaken at the defined timeframes for each of the indicators. The preparation involves defining detailed monitoring and evaluation timelines and milestones and ensuring the availability of all the resources required to support the monitoring and evaluation activities including the monitoring and evaluation teams and data collection tools. Depending on the timelines or reporting frequency set for each of the identified indicators, the indicators should be reviewed, and if necessary revised at the start of each next monitoring or evaluation cycle. The review and revision ensure that data is collected on the most relevant indicators during the monitoring or evaluation cycle.
11. Execute the monitoring and evaluation data collection activities and track indicator measures according to the DH maturity stage, timing for delivery of the defined results, defined indicators, frequency of measuring the results, and defined monitoring and evaluation timelines.
12. Analyze collected data and report on actual situation versus target DH adoption and results as per defined indicators (see example reporting tool in **Error! Reference source not found.**). The analysis may also include identification of causes of divergences in actual and target performance at each stage in the results chain for each timeframe of measuring results.

Table 20. Example of Digital Health monitoring and evaluation reporting tool

Result	Indicator	Reporting Frequency	Baseline (Period)	Reporting Period 1		Reporting Period 2	
				Target	Actual	Target	Actual

Digital Health Impact							
Impact 1	Indicator 1.1						
	Indicator 1.2						
Impact 2	Indicator 2.1						
	Indicator 2.2						
Digital Health Outcomes							
Outcome 1	Indicator 1.1						
	Indicator 1.2						
Outcome 2	Indicator 2.1						
	Indicator 2.2						
Digital Health Outputs							
Output 1	Indicator 1.1						
	Indicator 1.2						
Output 2	Indicator 2.1						
	Indicator 2.2						
Digital Health Inputs and Activities							
Input 1	Indicator 1.1						
	Indicator 1.2						
Input 2	Indicator 2.1						
	Indicator 2.2						

13. Engage stakeholders to agree on corrective actions to address divergence between target and actual results, and provide for management of changes in the DH implementation scope, if required, to implement agreed corrective actions (MoH-Uganda, 2016; WHO & ITU, 2012).

14. For indicators that may be unrealistic or unachievable within the required timeframes, engage stakeholders to review and agree on re-fined indicators, targets and timeframes for consideration in the next round of results measurement.

COMPONENT 6: DH ENTERPRISE ARCHITECTURE GOVERNANCE MODEL

Architecture Governance is the practice by which Enterprise Architecture and other architectures are managed and controlled at an enterprise-wide level (Josey et al., 2018). It encompasses a series of processes, cultural orientation, and a set of owned responsibilities that ensure the integrity and effectiveness of the organisation's architecture.

Figure 7 illustrates the Digital Health Enterprise Architecture Governance structure based on practices for architecture governance proposed by TOGAF (The Open Group, 2018a) and leverages the Digital Health Governance structures highlighted in the Uganda National eHealth Strategy 2017-2021(MoH-Uganda, 2016) . The model highlights the governance structure and processes required to support the implementation and use of Digital Health in

Uganda's Health System. The organisation structure represented in **Figure 7** comprises five levels, including; MoH Senior Management, Health Information, Innovation and Research Technical Working Group (Architecture Review Board), Division of Health Information Management, the Digital Health Enterprise Architecture Program Office, and Digital Health Communities of Practice. Each level has specific roles and responsibilities in the development and implementation and use of Digital Health.

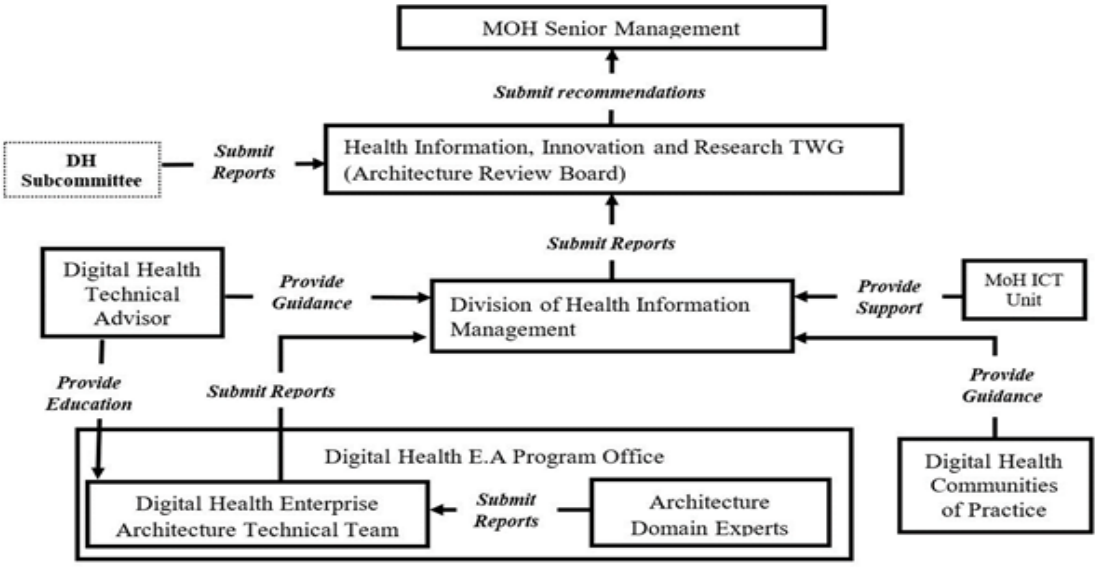


Figure 7. Digital Health Governance structure

Description, Roles, and Responsibilities of DHEAG in Health Organisations

(1) MoH Senior Management (Exists)

MoH Senior Management shall be the topmost decision-making body on all matters relating to Digital Health at the Ministry of Health. They shall be responsible for providing the governance to make Enterprise Architecture work within Uganda's health system. MoH Senior Management shall oversee all Digital Health Enterprise Architecture activities, including understanding and directing the linkage among MoH Health Sector Development Plan, MoH Digital Health Strategic Plan, business transformations, information governance transformations, and technology directions and investments across Uganda's health system. They will also act as vocal and visible champions for Enterprise Architecture initiatives within Uganda's Health sector and shall approve all project deliverables.

Roles and Responsibilities

- Approve Digital Health architecture standards, policies, and contracts.
- Approve Digital Health Enterprise Architecture Roadmap and promote it among all Digital Health stakeholders.
- Approve Digital Health Architecture deliverables.
- Approve funding for the Digital Health Enterprise Architecture activities.

- Approve the Digital Health Enterprise Architecture framework.
- Approve the Digital Health Enterprise Architecture Metamodel and Guidelines for Enterprise Architecture introduction.
- Provide strategic direction for the Digital Health Enterprise Architecture activities.
- Ensure the alignment of the Enterprise Architecture initiatives with both the National Health Sector Development Plan and Uganda National Digital Health Strategy.

(2) Digital Health Technical Advisor (Proposed)

The Digital Health Technical Advisor will serve as an expert who understands what it takes to develop, deliver and maintain high-quality Digital Health Enterprise Architecture. The Digital Health Technical Advisor shall be responsible for providing education to the Digital Health Enterprise Architecture program office. Additionally, the Digital Health Technical Advisor shall provide technical advice regarding Digital Health Enterprise Architecture implementation to the Division of Health Information Management.

Roles and Responsibilities

- Provide strategic direction to the Health Information, Innovation and Research (HIIRE) team to implement the DH Enterprise Architecture Framework.
- Guide Division of Health Information (DHI), HIIRE team, and MoH Senior Management on all issues that relate to Digital Health.
- Advocate and educate DH stakeholders on enterprise architecture and its benefits.
- Provide advice and training to all MoH internal Digital Health stakeholders on the current state of Digital Health technologies, policies, and functionalities.
- Assist with identifying and evaluating Digital Health solutions that will enhance the business processes of Uganda's health system.

(3) Health Information, Innovation and Research Technical Working Group (Exists)

The Health Information, Innovation and Research (HIIRE) Technical Working Group (TWG) is a multi-sectoral body responsible for providing technical advice to MoH and stakeholders on implementing the DHEAF framework. They will act as the Architecture Review Board (ARB) for all DH Enterprise Architecture artefacts. Within HIIRE, there shall be an Architecture sub-committee responsible for providing technical advice on EA. The committee will constitute individuals knowledgeable in EA who will be responsible for providing technical advice relating to all DHEA artefacts and deliverables.

Roles and Responsibilities

- Review all architecture artefacts/deliverables and make recommendations to MoH senior Management.
- Enforce compliance to Digital Health Enterprise Architecture and grant dispensations where necessary.
- Improve maturity levels of architecture discipline within Uganda's healthcare system.

- Ensure that the adoption of the discipline of architecture-based development is across the health sector.
- Monitor and control the Architecture Contracts.
- Resolve escalated ambiguities, issues, or conflicts.
- Considering policy (e.g., schedule, Service Level Agreements (SLAs), etc.) changes where similar dispensations are requested and granted.
- Providing a fundamental control mechanism for ensuring the effective implementation of the Digital Health architectures.

(4) Division of Health Information (DHI) Management (Exists)

The Division of Health Information (DHI) Management is a National Digital Health entity within the Ministry that coordinates and oversees Digital Health investment. In addition, it is responsible for reviewing and monitoring Digital Health strategy outcomes and developing strategic recommendations and priorities for consideration by the National Digital Health Steering Committee.

Roles and Responsibilities

- Provide strategic direction to the Enterprise Architecture Program Office.
- Advocate and educate Digital Health stakeholders (Patients/Clients, Heath Practitioners and Managers, Social Care Practitioners, Health Insurance organisations, Health researchers, and Health Development Partners) on enterprise architecture and its benefits.
- Market the benefits of enterprise architecture via collaborative forums.
- Prepare an implementation plan for Digital Health Enterprise Architecture Framework.
- Coordinate the development of segment and capability architectures across the health sector.
- Preparing and implementing the strategy for stakeholder management and engagement.

(5) Digital Health Enterprise Architecture Program Office (Proposed)

The DH Enterprise Architecture Program Office will be a permanent unit under the Division of Health Information (DHI) Management. The purpose of the program office will be to cultivate the culture of Enterprise Architecture practice throughout Uganda's health system.

Composition of Digital Health Enterprise Architecture Program Office

The composition of the Digital Health Enterprise Architecture Program Office includes:

- Manager, Enterprise Architecture
- Enterprise Architect(s)
- Domain Architect(s) (Business, Data, Application, Technology and Security)
- Enterprise Architecture Standards Specialist(s)

- Enterprise Architecture Policy Specialist(s)

Roles and Responsibilities

- Promote and support the MoH in the adoption and implementation of Enterprise Architecture practice.
- Coordinate and manage the Digital Health Enterprise Architecture Program, Digital Health Communities of Practice, Digital Health Enterprise Architecture Governance processes, and Architecture Repository.
- Ensure that DH Enterprise Architecture programs/projects are carried out consistently and successfully in compliance with standards, procedures, and strategies.
- Provide education on DHEA Framework, Standards, and Policies.
- Investigate performance issues of the Digital Health Enterprise Architecture initiatives and communicate early warning signs of the troubled areas.
- Ensure quality control, quality assurance, and process coaching. The Program office will inspect Digital Health Enterprise Architecture artefacts/ deliverables and provide coaching to Digital Health projects teams requiring additional support.
- Identify Enterprise Architecture risks and propose mitigation measures.
- Develop Enterprise Architecture Standards. They can work in conjunction with DH stakeholders to develop the standards.
- Develop Enterprise Architecture Policies. As part of their mandate to oversee that the policies are developed.

(6) Digital Health Communities of Practice (Exists)

The Digital Health Communities of Practice is a group of architects and other information technology and subject matter experts with shared interests and shared concerns and passion for Digital Health. This group will ensure the proper development and evolution of various Digital Health Enterprise Architecture artefacts and deliverables. In addition, the Digital Health Communities of Practice will purely play an advisory role in all Digital Health Enterprise Architecture initiatives.

Roles and Responsibilities:

- Influence the practice of EA by advising the Health Information, Innovation and Research (HIIRE) Technical Working Group in the development of Digital Health implementation plans.

Digital Health Enterprise Architecture Governance Processes

Architecture Governance processes are a set of activities that an organisation executes to support decision-making and accountability during the implementation of an architecture (Josey et al., 2018). The Digital Health Enterprise Architecture governance processes are intended to help identify, manage, audit, and disseminate all information related to architecture contracts and implementation management. In addition, these processes are designed to ensure monitoring of all architecture artefacts and contracts, principles, and operational-level agreements generated by Digital Health initiatives.

Architecture Policy Management and Take-on

All architectural amendments, contracts, and supporting information must come under governance through a formal process to register, validate, ratify, manage and publish new or updated content (The Open Group, 2018b). This requires that the MOH enacts effective architecture policies to guide all Digital Health Enterprise Architecture initiatives. For purposes of effective policy management and take on, MoH should adhere to the following:

- MoH Senior Management shall have the authority to issue architecture policies. This will, however, only be done after an appropriate review by MoH Senior Management and HIIRE TWG.
- MoH Senior management shall ensure timely communication of architecture policy changes. Timely communication of architectural policy changes will strengthen a culture of policy adherence among Health organisations.
- All changes to architecture policies shall be documented to track all changes. Records should specify who made the change, why they made it, and when the change was made.
- The MoH should put a central place (repository) where DH Organisations can easily access all architecture policies. Clear and well-organised architecture policies provide little benefit if the people who need them cannot access them. Therefore, MoH should ensure that all EA policies are accessible to the public through the MoH DH repository.
- The MoH should put a feedback mechanism for Digital Health stakeholders' comments on the architecture policies. A culture that does not readily accept stakeholders' comments will likely produce a substandard set of architecture policies.
- The MoH should regularly review all architecture policies. The review dates should be agreed upon when the policy is first created. A key element of effective policy management is an ongoing commitment to review and update all policies before they become outdated periodically.
- Drafting or revision of architecture policies should follow a formal process. Following a formal process result in policies that are consistent and reflect the needs of stakeholders (Hudson et al., 2019). **Figure 8** shows an 8-step process that shall be followed to develop or review architecture policies. This process borrows the best practices for stakeholder involvement highlighted in the WHO National eHealth Strategy toolkit (WHO & ITU, 2012).

Architecture Compliance Review

An *Architecture Compliance Review* is a scrutiny of the compliance of a specific project against established architectural criteria, spirit, and business objectives (The Open Group, 2018a). Confirming the compliance of individual DH projects with the Digital Health Enterprise Architecture framework is an essential aspect of Architecture Governance. Therefore, the Division of Health Information Management shall periodically carry out compliance reviews for all Digital Health initiatives to ensure conformance to the Architecture Vision, Principles, and Standards. Architecture compliance reviews should be held at appropriate project milestones. The most appropriate times are when the architecture is taking shape but when there is still time to correct any errors or shortcomings in the architecture effort. **Figure 9**

shows the compliance review process for all Digital Health Projects. The compliance review process is adopted from the TOGAF and contextualised for Uganda.

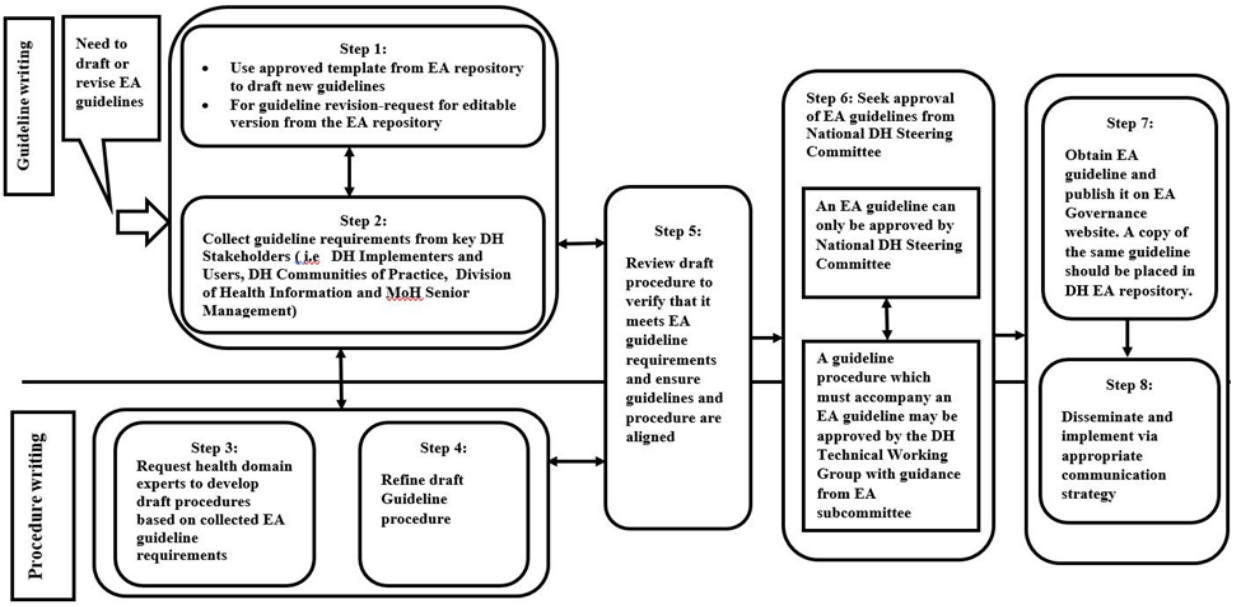


Figure 8. Architecture Policy Development Process (WHO & ITU, 2012)

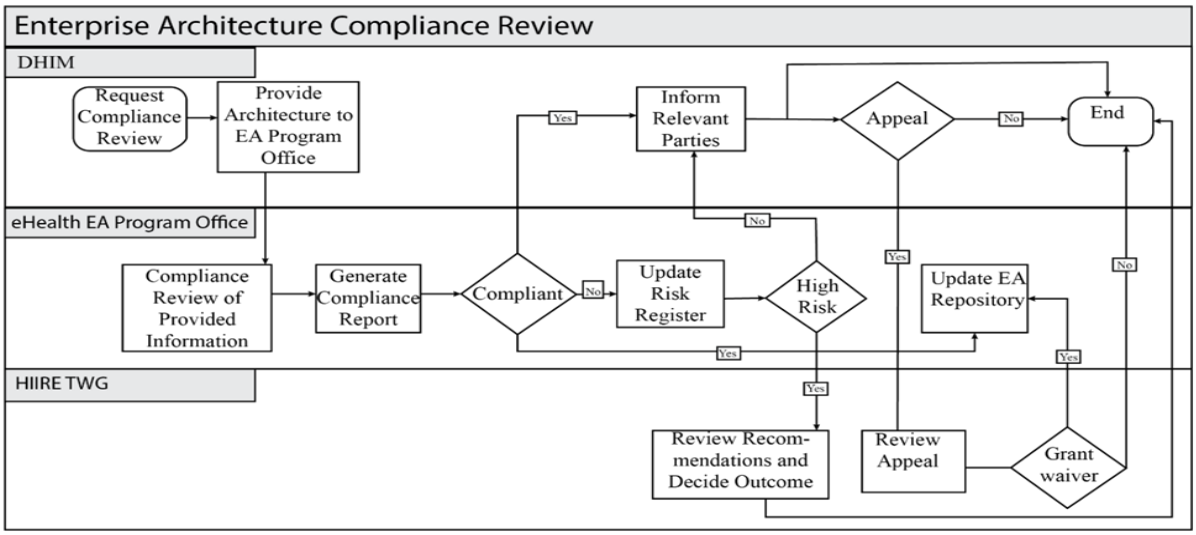


Figure 9. Architecture Compliance Review Process (The Open Group, 2018)

Description of the architecture compliance review process

The compliance review process for all Digital Health projects shall follow these steps:

1. The Division of Health Information (DHI) Management, which is the overall overseer of all Digital Health initiatives in the MoH, shall request the Digital Health Enterprise Architecture Program Office to undertake a compliance review for a Digital Health initiative that is under execution.
2. The Division of Health Information shall provide the Digital Health EA Program office with all pertinent architecture information required for the review.

3. The EA program office shall conduct the compliance review based on information provided by the DHI and any other information that may be available in the Ministry's Digital Health Architecture repository. Compliance reviews shall be carried out every quarter (i.e., every 3 months).
4. On completion of a compliance assessment, a Compliance Review report shall be forwarded by the Digital Health EA Program Office to the DHI, who will liaise with the relevant Digital Health project to inform them of the outcome.

    - If the architecture of the Digital Health project is fully compliant, the DHI will allow the project to continue.
    - If the architecture is partially compliant, the Digital Health project shall be required to submit a reworked architecture within one month.
    - If the architecture is non-compliant, the DHI shall forward the review report to HIIRE TWG for further consideration. In this case, a risk is added to the appropriate risk register; an assessment shall be carried out to determine its likelihood and impact. If the likelihood and impact of the risk are high, HIIRE TWG may issue recommendations that may include suspension of work until the risks have been effectively mitigated.

Request for Exception (Dispensation)

There may be cases in which a Digital Health initiative or a subject area (design, operation, service level, or technology) does not comply with the DH Enterprise Architecture Framework. These non-compliance cases may either be known at the initiation stage or are revealed through the Architecture Complains reviews. In cases where the non-compliant subject area, despite best efforts utilized, cannot comply with the Digital Health EA Framework and needs more time to comply, dispensation may be requested for the subject area (The Open Group, 2018a). However, to determine a dispensation requirement, a Health organisation shall discuss the dispensation requirement with the Digital Health EA Program Office. If the request is required, the health organisation will be allowed to submit a dispensation request to the Digital Health Program Office. For all DH projects, requests for exception to any architectural activity, policy, or standard shall follow the following process:

Step 1. Submit and process Requests at Digital Health Enterprise Architecture Program Office

Requests for exceptions shall first be submitted to the Digital Health Enterprise Architecture Program Office. The submitted request shall be recorded into the Enterprise Architecture Dispensation Register and allocated a unique reference identifier. Requests shall include:

- A description of the Digital Health project and its timeline.
- A description of the specific exception sought.
- A statement of the reasons for the exemption.
- A description of the steps taken to eliminate the need for the exception in the future.

Requests for exemption shall be allowed to be submitted at any time in the project's progress. However, the turnaround time shall be determined at the project level. They shall specifically include a Request for Proposal (RFP) response evaluation to determine whether to consider a particular response. The appropriate subject matter experts should assess each request, and

the assessment shall include an evaluation of the health organisation's ability to implement the Digital Health Enterprise Architecture Framework.

Any issues or risks that arise during evaluation shall be negotiated with the submitting health organisation. After the assessment, the assessor shall provide a written recommendation to the relevant governing bodies for consideration. The recommendations should include any outstanding issues and risks, and conditions on granting the dispensation. The recommendations may include a deadline for removing the need for the exception, constraints on future projects, or similar terms.

Step 2: Appeal (if necessary) request at Division of Health Information Management
If the Digital Health EA Program Office does not grant the request and a particular Digital Health stakeholder is dissatisfied, the decision may be appealed to the DHIM. The DHIM shall consider the request at the next regular meeting (as defined by MoH's Division of Health Information) or, if necessary, at a special meeting. The DHIM may request additional information in order to make its decision.

Step 3: Re-appeal (if necessary) at HIIRE Technical Working Group
If the DHIM does not grant the request, the Digital Health project may submit an appeal to the HIIRE Technical Working Group. The HIIRE TWG decision shall be final.

Risk Management Process
There will always be risks with any digital transformation effort (The Open Group, 2018a). Therefore, it is important that risks are classified, identified, and mitigated early enough so that they can be tracked through a formal risk management process (Josey et al., 2018). The early identification of potential problems allows the creation of plans to reduce their potential adverse impact (Barateiro et al., 2012). Therefore, risk management shall be an integral part of all Digital Health initiatives. The goal is to define prevention and control mechanisms to address the risks attached to specific activities and valuable assets. Therefore, all Digital Health organisations shall be required to implement a risk management process. Where such a process exists but is insufficient, it can be extended by best practices stipulated in ISO 31010 2019 Risk management framework or The Open Group Enterprise Architecture Framework. Key steps to the risk management process should include classification, identification, analysis, evaluation, and treatment. Continuous monitoring and review should also be carried out to audit the behavior of the whole environment allowing, for instance, the identification of changes in risks or the suitability of implemented risk treatment procedures and activities. Also, there should be continuous communication and consultation with key stakeholders. throughout all the steps.

Architecture Repository Management
The Architecture Repository is a software tool that stores the essential architectural inputs and outputs, including Architectures themselves, the elements of which they are composed, standards, references, principles, and the Governance Register (The Open Group, 2018a). **Figure 10** provides a structural framework for the DHIM Architecture Repository, which will allow the division to distinguish between different types of architectural assets that will be realised by the various digital transformation efforts within Uganda's health sector. Six classes of architectural information shall be held within the MoH Enterprise Architecture

Repository. These include; the Digital Health Enterprise Architecture framework, Digital Health Governance framework, Digital Health Architecture Landscape, Standards, Reference models, records of governance activity, Digital Health requirements for Uganda, and Solution Building Blocks (SBBs) supporting the Architecture Landscape.

Description of Contents of Sections of the Repository

Architecture Metamodel – stores the DH Enterprise Architecture Framework for Uganda.

Architecture Capability – stores the parameters, structures, and processes that support governance of the Architecture Repository.

Architecture Landscape – stores architectural views of the state of the MoH Enterprise Architecture descriptions at particular points in time. The Architecture Landscape shall be divided into three levels, namely; *strategic architecture*, which shows the long-term summary view of the MoH Enterprise Architecture; *segment architecture*, which provides more detailed operating models for different healthcare domains; and *capability architecture*, which shows in detail how a unit of capability is going to be realised.

Standards Information Base – stores all standards with which new architectures must comply, including data, communication and infrastructure standards, application standards, selected products and services from suppliers, or shared services already deployed within MoH.

Reference Library – stores guidelines, templates, patterns, and other forms of reference material that can be leveraged to accelerate the creation of new architectures for health organisations within the MoH.

Governance Log – stores all records of governance activity related to the Digital Health Enterprise Architecture. The Governance log holds all architecturally significant decisions made, Compliance assessments, Capability assessments, and Performance assessments.

Architecture Requirements – stores all authorised architecture requirements which have been approved by the HIIRE Technical Working Group (Architecture Review Board).

Solutions Landscape – stores Solution Building Blocks (SBBs) supporting the Architecture Landscape which have been planned or deployed by the health organisation.

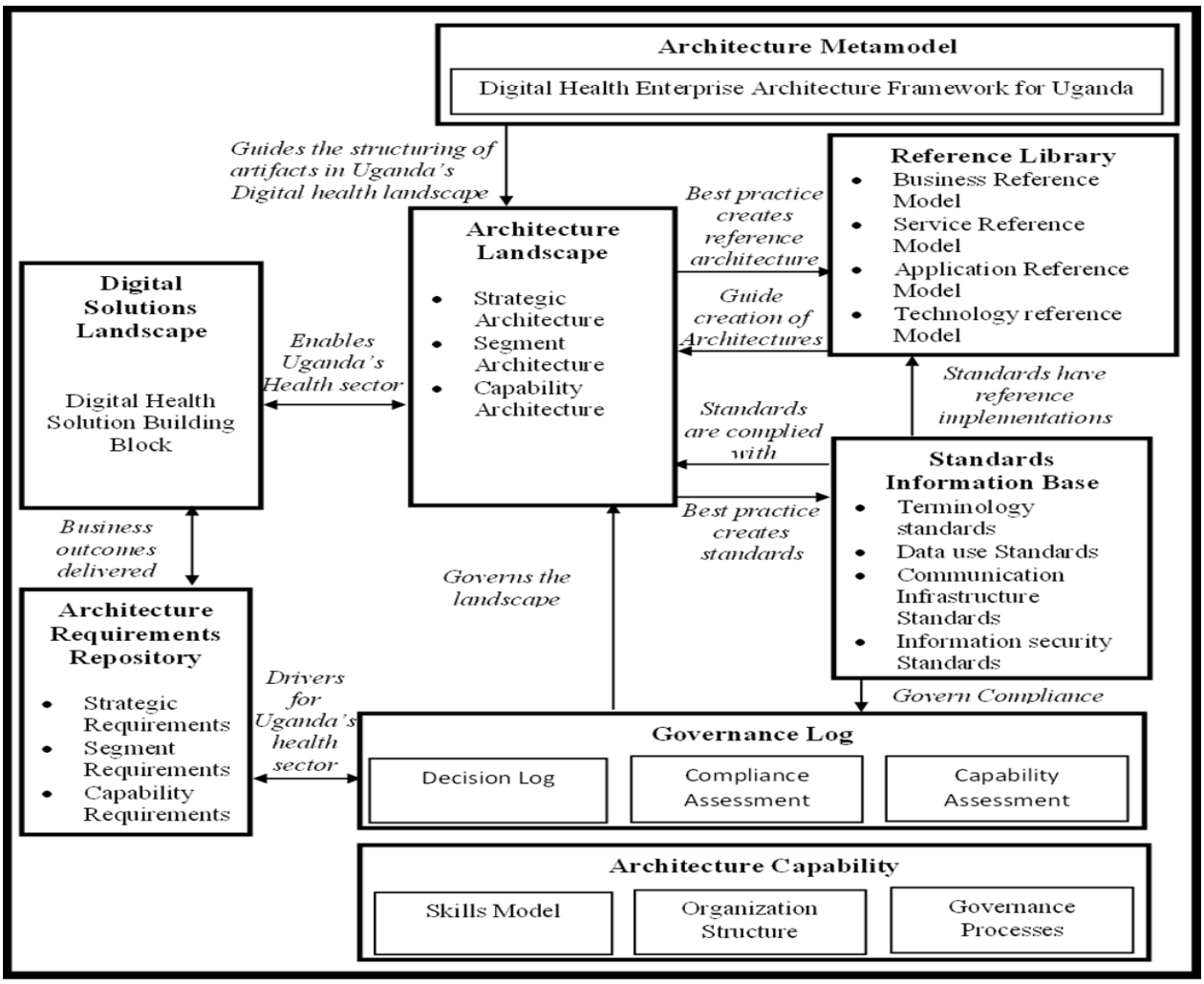


Figure 10. MoH Architecture Repository

COMPONENT 7: DIGITAL HEALTH SECURITY ARCHITECTURE

Privacy relates to the metadata that allows for geo-positioning of the digital health solution when in use. ***Confidentiality*** relates to the obligation of the digital service provider or other third-party user to protect the disclosure of either the content or metadata without explicit permissions from the client. ***Security*** relates to adoption and application of reasonable, technical and organisational measures to prevent loss, damage or unauthorised destruction and unlawful access to processing of the personal data.

The ***Digital Health Information Security Architecture*** (DHISA) intends to strengthen security regards; *Confidentiality* (ensuring that information is not made available or disclosed to unauthorised entities), *Integrity* (protecting the accuracy and completeness of information), and *Availability* of health data/information (being accessible and usable when an authorised entity demands access) (ISO/IEC 27000 standard) held by Digital Health systems in Uganda.

The DHISA as presented in **Figure 11** is based on Sherwood Applied Business Security Architecture (SABSA) framework for enterprise security architecture and the Principles for

Digital Development which outline best practices for digital health programming. SABSA is a framework and methodology for enterprise security architecture and service management, and it integrates freely with TOGAF, the foundational framework for the Digital Health Enterprise Architecture Framework.

The DHISA comprises three main components that support each other to realize *Confidentiality*, *Integrity*, and *Availability* of health information. Additionally, DHISA includes all security considerations related to governance, technology, and operations that are required to protect the information assets of MoH. Specifically, the components are intended to ensure security of health information held by Digital Health systems by providing accountability and assurance.

1. **Security Drivers** – these are elements (internal and external) that can act as a source of information security for an organisation. DHISA highlights four key security drivers that Health organisations should focus on when identifying security requirements. Business requirements and opportunities are the key sources of internal security requirements. These have the service-level business requirements that must be met to effectively and efficiently provide services to clients. External security requirements may be derived from threats and the need to comply with legal and regulatory requirements. Privacy and confidentiality are key examples of functional requirements driven by legal requirements.

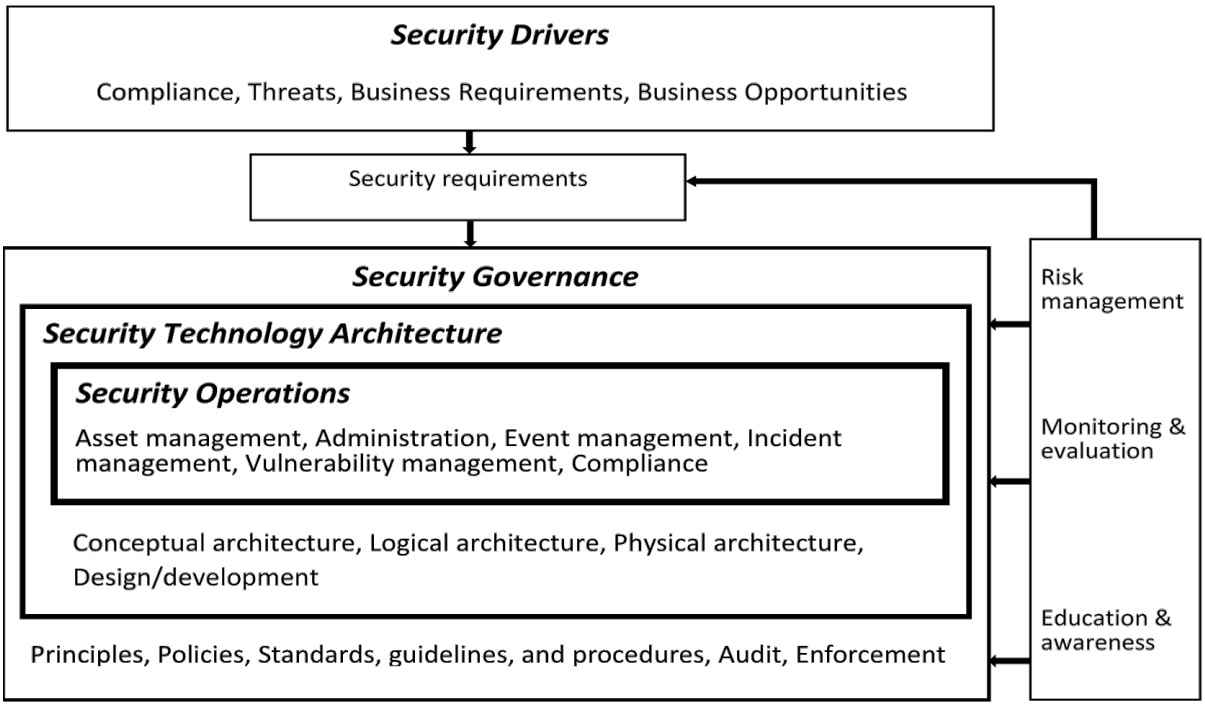


Figure 11. Digital Health Information Security Architecture

Security Requirements – these represent an information security functionality that ensures that the security properties of an Information system are being satisfied (Harris & Maymi, 2019). Security requirements drive the development of a Health organisation's security governance as well as the entire security program. Security requirements of Digital Health systems should be defined in terms of availability, integrity, and confidentiality.

Monitoring and Evaluation – this is the ongoing assessment of a Health organisation's compliance with DHISA and responding to changes that may impact any aspect of the security governance processes and policy framework.

Risk management – this is the process of determining the acceptable level of security risk at various points in health organisations DH system and implementing the optimal level of management and technical control.

Education and awareness – these are programs that create awareness about current information risks and security practices so that DH users are empowered to protect the confidentiality, integrity, or availability of systems and data.

Security Governance – these are principles, policies, standards, guidelines, and procedures that allow the security goals to be set, expressed, and communicated throughout the different levels of a Health organisation. It grants power to entities needed to implement and enforce security and provides a way to verify the performance of these necessary security activities.

Security Technology – this is a set of conceptual diagrams and blueprints that document what the resulting security system will look like from various perspectives, including; conceptual, logical, and physical architectures.

Security Operations – these are security considerations for the day-to-day operations of the security services and supporting infrastructure. They include;

> Asset management – a component and process for maintaining the inventory of hardware and software assets required to support device administration, compliance monitoring, vulnerability scanning, and other elements of security operations.
> Administration – the process for securing the organisation's operational digital assets against accidental or unauthorised modification or disclosure.
> Event management – the process for the day-to-day management of the security-related events generated by a variety of devices across the operational environment, including security, network, storage, and host devices.
> Incident management – the process for responding to security-related events that indicate a violation or imminent threat of a breach of security policy (i.e., the organisation is under attack or has suffered a loss).
> Vulnerability management – the process of identifying high-risk infrastructure components, assessing their vulnerabilities, and taking the appropriate actions to control the level of risk to the operational environment.
> Compliance – the process of ensuring that the deployed technology conforms to the organisation's policies, procedures, and architecture.

2. **Security Governance** – establishes a governance model that Health organisations can use to assure that their DH information security strategies are aligned with and support business goals of MoH and are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility.

Principles – are general rules and guidelines intended to be enduring and seldom amended that inform and support how an organisation sets about fulfilling its mission (Josey et al., 2018). All policies, standards, architectures, designs, operations, and other components of

Digital Health should always be aligned to established governance principles unless a governance body has granted an exception. Depending on the Health organisation, governing principles may be established at one or more levels. When adapting security principles to their needs, Health organisations should ensure that they are aligned with the high-level IT principles, which guide the use and deployment of all IT resources and assets across the enterprise. The DHEAF provides a list of security principles that Health organisations can adopt for their environments.

Policies – are governance tools used to enforce an organisation's guiding principles (Harris & Maymi, 2019). They define the authorizations and a program of actions adopted by an organisation to govern the use of technology in specific areas of management control and are established and maintained through standards, guidelines, and procedures in accordance with related legal and business principles. Health organisations should define a set of policies for information security and have them approved by their respective management. The information security policies should contain statements concerning definition of information security, objectives and principles to guide all activities relating to information security; assignment of general and specific responsibilities for information security management to defined roles and, processes for handling deviations and exceptions. Additionally, security policies should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Standards, Procedures and Guidelines – these are mandatory activities, actions, or rules. Policies should be implemented through; technical standards (mandatory directives that must be adhered to by all users), guidelines, and procedures (describe how to achieve the standard or guideline), which are distinguished as follows:

Enforcement – the process of ensuring compliance with policy. For all Health Organisations, enforcement of information security should be accomplished through a combination of technical controls, process and procedure controls, and management controls. Controls should be built into the implementation of technical standards and procedures. Management controls should provide for discretionary invocation of enforcement processes (such as disciplinary actions) as a result of security events or incidents.

Audit – an Information security audit is an organized, quantifiable technical assessment of how the organisation's security policy is employed (Onwubiko, 2009). Health organisations are encouraged to establish their own security audit frameworks and have them formally approved by relevant authorities. The framework comprises; the security policy (that defines acceptable use, technical controls, management standards and practices), audit policy (that specifies what needs to be audited), processes (organisation processes around security, procedures needed to protect valued assets), and regulatory compliance (that stipulates acceptable regulatory and security compliances).

3. **Security Technology Architecture** – focuses on sophisticated security infrastructures that support the DH applications. The model is described at four levels of abstraction; conceptual architecture, logical architecture, physical architecture and design/development.
    a. ***Conceptual Architecture*** – is a generic technical framework for policy-based security services. It decomposes policy management and security services to

specific conceptual services. The conceptual architecture should clearly state the overlap between policy management and runtime security services management splitting it into identity management, access management, and configuration management services, which represent three roles of the tactical security.

Identity management services – responsible for assigning and maintaining digital identities and associated attributes across the electronic computing environment and for deleting identities when they no longer represent valid users of the environment.

Access management services – responsible for assigning and maintaining resource access privileges across the electronic computing environment and for terminating those privileges when they are no longer required. Access management services may encompass a variety of components such as access policy definition, account creation, and access control list (ACL) maintenance.

Configuration management services – responsible for consistently setting and maintaining the security configuration across the electronic computing environment. Configuration management is where the eHealth security technology extends to include distributed components for all security services. Configuration of the various security services should include; boarder protection, threat detection, content control, auditing, cryptography, and even configuration management itself.

b. ***Logical Architecture*** – identifies discrete logical services and their relationships at the level required to determine what the health organisation needs to build or buy in order to construct a set of identity management services for the digital health environment. It entails;

Human resource system – provides administrative feeds to create or update internal user identities in the internal entities directory.

External identity administration system – creates or updates external user identities in the external entities directory on behalf of affiliated enterprises. User administration may be delegated to an administrator at the affiliate enterprise site.

Identity registration and vetting functions – provide the means for establishing digital identities for persons that might not go through the human resource system, such as contractors or consultants. Additional functions may be included to support special identity attributes, such as security clearances or citizenship, which may be provided by external organisations other than internal human resource system.

c. ***Physical Architecture*** – physical implementation of servers, software, network connections, etc., of identity management environment described by the logical architecture. This architecture environment should have multiple documents, including; Software component layering on servers and network topology diagrams, all network addresses of Domain Controllers in an environment, and documentation of the configuration settings for software components.

d. ***Design and Development*** – these identify the types of guidance that organisations may want to provide to those responsible for design, development, and deployment of applications. Design and development guidance may range from overall process guidelines to specific guides, templates, and tools. These may include design patterns, code samples, reusable libraries, and testing tools. All of these are aimed at effective utilization of information security architecture and effective integration into the environment. This guidance can be applied to

components or applications built in-house as well as commercial off-the-shelf (COTS) applications selected for integration.

4. **Security Operations** – these define the processes required to support a policy driven security environment. This domain consists of two key processes major categories; one category comprises the administration, compliance, and vulnerability management processes required to ensure that the technology as deployed conforms to policy and provides adequate protection to control the level of risk to the environment; while the other category consists of the administration, event, and incident management processes required to enforce policy within the environment. Further guidance on how these can be addressed can be found in ISO 27002. The security operations domain of MoH's DHISAF has a strong dependency on asset management. They entail;

Asset Management – a component and process for maintaining the inventory of hardware and software assets required to support device administration, compliance monitoring, vulnerability scanning, and other elements of security operations. Common components include a repository of hardware and software assets (including the configuration and usage information), a capability to discover assets as they are added to the network, and reporting capabilities (ISO/IEC, 2018). This information may be used for activities e.g., contract renewals, software license compliance audits, and cost reduction activities. This requires that health organisations identify all assets associated with information and processing facilities and also define appropriate protection responsibilities. An inventory of these assets should be drawn up and maintained on a regular basis. ISO/IEC 27005 provides examples of assets that might need to be considered by health organisations when identifying assets.

Security Administration – the components and processes for securing the health organisation's operational digital assets against accidental or unauthorised modification or disclosure. This is accomplished by planning, coordinating, and implementing the Digital Health systems and best practices required to create and maintain secure access to resources and protect the integrity of the system and device configurations. Security administration comprises two primary sub-components namely; 1). Identity management (responsible for the creation, modification, and termination (inactivation or deletion) of digital identities, including the workflow process for managing both identity and access management information. It is also responsible for management of authentication tokens and certificates); 2). Device configuration (responsible for technical standards instantiation at the device level. It is also responsible for ensuring that updates to the actual devices are reflected in the asset database).

SECTION 2: DIGITAL HEALTH STANDARDS FOR UGANDA

2.1. DATA AND INTEROPERABILITY STANDARDS

Figure 12 shows the contextual data and interoperability standards that shall be applied to ensure that the patient (health) data collected, information processed, shared, and stored are in formats that support both semantic and syntactic interoperability. Data and interoperability standards include medical coding, data exchange and sharing standards. These comprise of six (6) dimensions; Patient Identification, Health Information Exchange Registries, Compliance, Management and Communication of Medical Imaging Data, Health Information Systems, Digitization of Health Information, and the crosscutting Security and Privacy for Data and Training and capacity building standards.

These standards are contextualised from several resources including; the Uganda Privacy Act, (HL7) Health Level Seven (Lin et al., 2012), (FHIR) Fast Healthcare Interoperability Resources (Lin et al., 2012) and (DICOM) Digital Imaging and Communications in Medicine (Greenwell & Salentine, 2018; Saripalle et al., 2019), (HL7 Service-Aware Interoperability Framework: Canonical Definition Specification, Release 2 Draft Standard for Trial Use (2012); HL7_FHIR_DCOM Standards, 2022), Interoperability Framework. The e-Government Interoperability Framework Reference Architecture (GIRA) for Uganda was also used as a reference architecture focused on the design of end-to-end interoperable digital public services. The GIRA is composed of the most salient Architecture Building Blocks (ABBs) needed to promote cross-sector interactions between Ministries Departments, Agencies (MDAs) and Local governments (LGs).

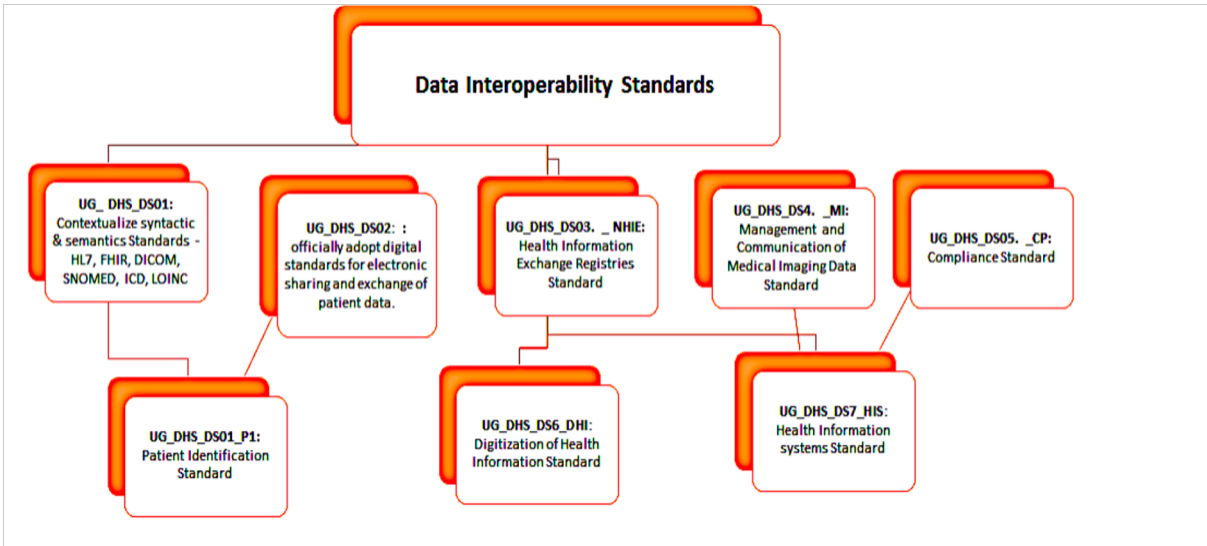


Figure 12. Contextualised Data and Interoperability Standards

UG_DHS_DS01_P1: Patient Identification

> ***Statement***: Establish a unique, standardised, comprehensive, and comprehensible Electronic Medical Record (EMR), Electronic Health Records (EHR), and Personal Health Record (PHR).

Rationale

UG_DHS.DS01_P1_Rt1: A unique identifier in eHealth services will provide for accurate identification of a given patient across a continuum of care to address the priority business needs of patients/clients, healthcare providers, and healthcare managers by improving efficiency, effectiveness, data management and utilization, resource planning. All health record systems must therefore adhere to standards for capturing information related to patient demography and identifiers.

Implementation Specification(s)

UG_DHS_DS01_P1_Rt1_IS1: Adopt and enforce a Unique Identifier for every Patient/Client. This may include the National Identification Number (NIN) and the Legally Resident Alien Identification Number (AIN) as the Unique Identifier of every Patient/Client or any other nationally acceptable identifier in circumstances where patients/clients do not have NINs or AINs such as children and non-registered aliens.

UG_DHS_DS01_P1_Rt1_IS2: Identify and analyze all initiatives by different stakeholders towards the design of EMR, EHR, and PHR with a view of its utilization.

UG_DHS_DS01_P1_Rt1_IS3: Design, adopt and enforce EMR, EHR, and PHR that conforms to National and international standards.

UG_DHS_DS01_P1_Rt1_IS4: Monitor and evaluate the adherence and conformance to the unique identifier standard.

UG_DHS_DS01_P1_Rt1_IS5: All eHealth systems that collect patient level data should have provision for following minimum identifiers (e.g., Name, date of birth, gender, NIN etc.).

UG_DHS_DS02. _ NHIE: Health Information Exchange Registries Standard

Statement: Developing and maintaining comprehensive interoperable master lists of health facilities, providers, and patients/clients is a necessary step toward monitoring health infrastructure and services that form a core component of the national Health Management Information System (HMIS).

Rationale

UG_DHS_DS02. _ NHIE_Rt1: For a health record system to function properly in a larger ecosystem of other components there have to be communication protocols to enhance sharing of data to realize a continuum of care.

Implementation Specification(s)

UG_DHS_DS02. _ NHIE_Rt1_IS1: Provide a protocol for electronic exchange of data in healthcare environments.

UG_DHS_DS02. _ NHIE_Rt1_IS2: Data should be readily available and accessible as and when it is required by authorised users.

UG_DHS_DS02. _ NHIE_Rt1_IS3: Shall enable healthcare planning and financial management to ensure effective collection, allocation, and use of health financial resources at all levels by health plan priorities

UG_DHS_DS02. _ NHIE_Rt1_IS4: Shall define specifications for information object definitions, data structures, and their semantics, protocols for the exchange of medical information among imaging equipment and other healthcare applications, file format, and storage of medical images.

UG_DHS_DS02._NHIE_Rt1_IS5: Shall enable the exchange of clinical data between systems to support a central patient care system as well as a more distributed environment where data resides in departmental/decentralized systems.

UG_DHS_DS02._NHIE_Rt1_IS6: Enable the exchange of clinical and administrative data among healthcare applications in the form of patient demographics, health insurance data, clinical observations, appointment schedules, and patient referrals etc.

UG_DHS_DS02._NHIE_Rt1_IS7: Strengthen healthcare professionals' human resource management to ensure effective information management, assignment, development, and accountable use of health human resources at all levels following health plan priorities.

UG_DHS_DS03. _CP: Compliance

Statement: Establish an Intelligent and Integrated monitoring mechanism to ensure compliance across the health sector. Generate data for observation and clinically relevant events and encounters. This requires having a common semantic and syntactic logical information model and structural composition.

Rationale

UG_DHS_DS03. _CP_Rt1: Without the right data standards being implemented wrong communication will be realised in the whole ecosystem. Therefore, a health record system must conform to agreed standards.

Implementation Specification(s)

UG_DHS_DS03. _CP_Rt1_IS1: Generic implementation should be harmonized with the design requirements and preferred technology platforms.

UG_DHS_DS03. _CP_Rt1_IS2: Monitor systems against specifications for the structure and semantics of health data to support a common representation of recommended standards e.g., clinical summaries, discharge notes, and radiology reports, etc.

UG_DHS_DS03. _CP_Rt1_IS3: Establish a monitoring system to support inspection and compliance monitoring of electronic data, information and knowledge management, analysis and utilization System.

UG_DHS_DS4. -_MI: Management and Communication of Medical Imaging Data

Statement: This includes all health record management in terms of imaging modalities including radiography, magnetic resonance imaging (MRI), nuclear medicine, ultrasound, tomography, echocardiography, X-ray, CT, and other modalities used in radiology, cardiology, radiotherapy, ophthalmology, and dentistry.

Rationale

UG_DHS_DS4. -_MI-_ Rt1: For comprehensive handling and managing of images (series or single), waveforms (such as those in ECG/EEG), audio (such as those in digital stethoscope), and video (such as those in the endoscope, ultrasound, etc.) data in medicine. Where required and relevant, other features of standard such as services, display, print, and workflow may be implemented.

Implementation Specification(s)

UG_DHS_DS4.-_MI-_Rt1_IS1: Data elements must serve the purpose of documentary records of various diagnostic and prescriptive data or information generated.

UG_DHS_DS4. -_MI-_ Rt1_IS2: Medical equipment procured must comply with the universal format for PACS (picture archiving and communication systems) image storage and transfer Scanned or Captured Records:

- Image: JPEG lossy (or lossless) with size and resolution not less than 1024px x 768px at 300dpi
- Audio/Video file document Management formats should comply with Long-Term Preservation

UG_DHS_DS4. -_MI-_ Rt1_IS3: Where no maximum image resolution has been prescribed, a sufficiently acceptable limit may be used to avoid unnecessarily large files that do not aid in correspondingly better interpretation or analysis.

UG_DHS_DS4. -_MI-_ Rt1_IS4: Preference in the procurement of IT hardware and software for image data management shall be from an authorised dealer licensed and accredited by NITA-U or on the PPDA Register of Providers and comply to the DCOM/ PACS Standards.

UG_DHS_DS5_HIS: Health Information systems Standard

Statement: Establish mechanisms for implementing and adhering to set guidelines for all HIS solutions in the health sector

Rationale

UG_DHS_DS5_HIS_Rt1: The HIS guidelines will support the collection, quality review, aggregation and reporting of health-related data for clinical and system-wide use in a timely, and reliable manner.

Implementation Specification(s)

UG_DHS_DS5_HIS_Rt1_IS1: Define data, information and knowledge lifecycle responsibilities and requirements (e.g., Processes, Data Ownership / Stewardship, Audit, Creation and Collection, Analysis, Retention and Disposal, Data Quality, etc.).

UG_DHS_DS5_HIS_Rt1_IS2: Develop a "Right to Use" Policy - Defining the purposes for which health data can be used by providers in the direct delivery of care to the patient (e.g., "Need to Know" rules).

UG_DHS_DS5_HIS_Rt1_IS3: Develop Data, Information and knowledge Sharing Agreements. Defining the purposes for which health data may be shared between organisations and custodians, observing terms and responsibilities.

UG_DHS_DS5_HIS_Rt1_IS4: Define requirements for data collection, storage, analysis, and reporting and dissemination mechanisms.

UG_DHS_DS5_HIS_Rt1_IS5: Identify data sources, storage and flow patterns that enable timely and accurate collection and information exchange.

UG_DHS_DS5_HIS_Rt1_IS6: Develop a reporting process that is aligned to the requirements at all relevant levels.

UG_DHS_DS5_HIS_Rt1_IS7: Develop guidelines, SOPs, manuals for data use and utilization for ownership, usage to influence decision making processes at different levels (clinicians, data managers, clients, researchers, policy makers, partners etc.).

UG_DHS_DS6_DHI: Digitization of Health Information Standard

Statement: Establish an ICT infrastructure that forms the foundations for electronic communication and information/data sharing across geographical and health-sector boundaries. This includes the computing infrastructure, databases, directory services, network connectivity, and storage that underpin a national eHealth environment.

Rationale

UG_DHS_DS6_DHI_Rt1: Improving the quality of health care services in terms of efficiency, availability, accessibility, reliability and timeliness to ease interoperability of patient information across the health facilities.

Implementation Specification(s)

UG_DHS_DS5_HIS_Rt1_IS1: Establish a cost-effective and affordable ICT infrastructure to support communication and sharing of information/data across the continuum of care.

UG_DHS_DS5_HIS_Rt1_IS2: Strengthen the electronic health information system (HIS) to support evidence-based health care and decision making.

UG_DHS_DS5_HIS_Rt1_IS3: Enable electronic delivery and interventions of health services in line with the universal health coverage to all Ugandans.

UG_DHS_DS5_HIS_Rt1_IS4: Implement a National Minimum Health Care Package (UNMHCP) which includes promotive, preventative, curative, rehabilitative, and palliative care.

UG_DHS_DS5_HIS_Rt1_IS5: Shall enable electronic delivery of quality health care (mHealth, telehealth...) to all individuals in remote areas lacking needed expertise to reduce isolation, amplify the voices of the disadvantaged, and provide means to individuals to influence health systems.

UG_DHS_DS5_HIS_Rt1_IS6: Strengthen disease prevention, surveillance, and control by using hybrid ICT solutions to facilitate early detection and rapid reporting and response.

2.2 DIGITAL HEALTH COMMUNICATION INFRASTRUCTURE STANDARDS

The Digital Health Communication Infrastructure (DHCI) standards in **Figure 13** have five dimensions; hardware devices, connectivity and communication networks, applications and software, security and privacy, and facilitating resources (human resource, financial resource and electric power). These standards are contextualised from several resources including; Uganda Privacy Act, (ANSI/BICSI & Institute, 2018; EHRS FM R2; European Parliament, n.d.; European Parliament, Council of the European Union, 2004; European Union, 2015, 2019; Gary et al., n.d.; HHS Office of Civil Rights, 2013; HIPAA, 2013; ISO, n.d., 2017; ISO IS 17090-1 2013; ISO IS 17090-2 2008; ISO IS 22600-1 2014; ISO IS 27799 2008; ISO/IEC 27033-4:2014; ISO/HL7, n.d., n.d., p. 710781; ISO/IEEE, n.d.; ISO/TR, 2009; ITI Planning Committee, 2015; ITU-T, 2015; MoICT-Uganda, 2019; NITA-U, 2010; Singapore Ministry of Health, 2015; The Open Group, 2018; TR-42.1, 2017).

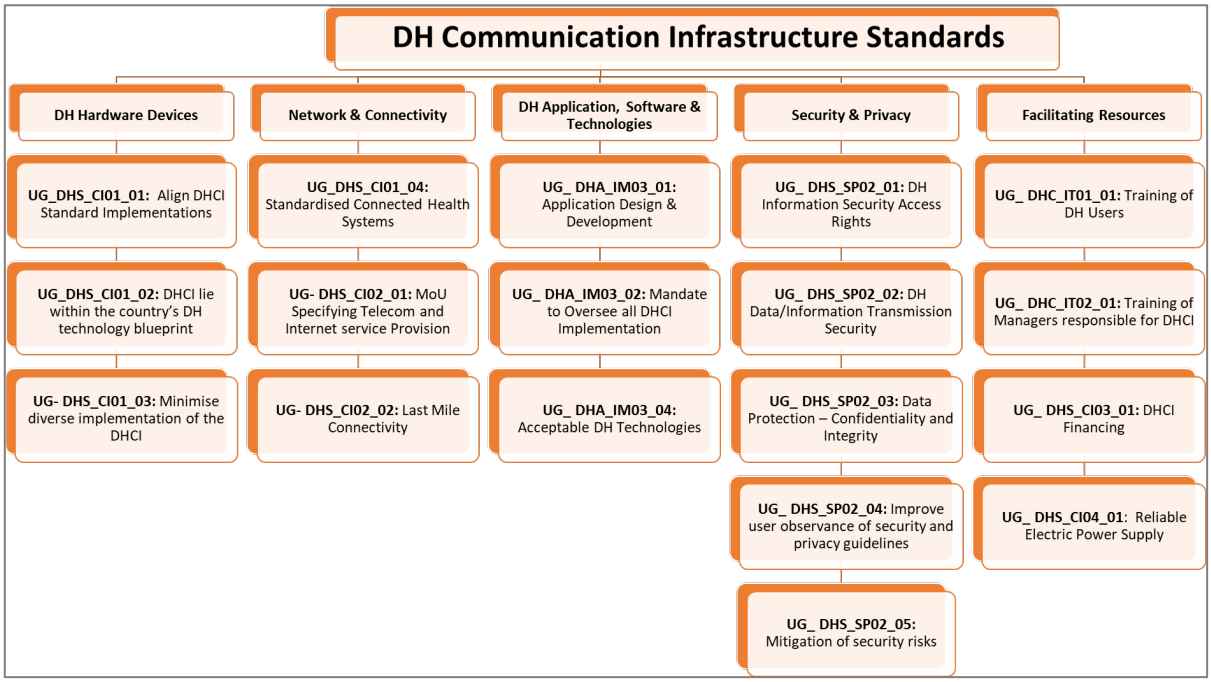


Figure 13. Contextualised DHCI Standards

2.2.1. HARDWARE DEVICES STANDARDS

UG_DHS_CI01_01: Align DHCI Standard Implementations

Statement: Critical areas and or changes in the DHCI are appropriately aligned to the country's digital health needs, eHealth strategy, and related policies.

Rationale

UG_DHS_CI01_01_Rt1: Changes in the DHCI are continuously researched, guided and well documented based on current DH user needs.

Implementation Specification(s)

UG_DHS_CI01_01_Rt1_IS1: MoH and participating health facilities and supporting organisations should procure and implement components of the DHCI following the MoH and related MDAs guidelines, including but not limited to;

(i) Requirements specifications for each component of the DHCI, technologies, and use, lie within Uganda's digital health technology blueprint.

(ii) The MoH and healthcare facilities/ organisations supporting health interventions procure and implement end-user ICT devices with adequate hardware (HW) and software (SW) specifications and networking devices to meet health data quality requirements.

(iii) MoH should ensure that appropriate data storage devices or data backup mechanisms are provided to all healthcare service delivery points. Additionally, MoH should ensure that each participant in the connected health system implements the different types of data backup procedures for differential and replication.

(iv) All healthcare service delivery points implement scheduled maintenance, repair, and environmentally friendly end-of-life and disposal of DHCI waste.

UG_DHS_CI01_01_Rt1_IS2: Government policy guidelines for operationalisation of the DHCI are implemented at all levels of Uganda's health system.

UG_DHS_CI01_02: DHCI lie within the country's DH technology blueprint

Statement

Minimum specifications of HW devices restrict implementations of the DHCI within the country's DH technology blueprint that assures healthcare facilities/ organisations participating in the connected health system establish a DH communication network with quality devices, data rate, and network services.

Rationale

UG_DHS_CI01_02_Rt1: Hardware devices should be able to support all forms of approved DH applications, health data and information being captured, processed, presented and or shared.

Implementation Specification(s)

UG_DHS_CI01_02_Rt1_IS1: ***Desktop Specifications*** - Processor family: I3 or Equivalent; Processor Speed: 2.2 Ghz; Cores: 2; Processor Cache: 2 mb; Processor Speed: 3 Ghz; Memory: 8 GB DDR4 Expandable; Storage: 256 GB SSD Expandable; Power Supply: 220 V; Network Controller: Ethernet and Wireless Support; Display: 17-inch Monitor, and HDMI/ VGA.

UG_DHS_CI01_02_Rt1_IS2: ***Laptop Specifications*** - Processor family: I3 or Equivalent; Processor Speed: 2.2 Ghz; Cores: 2; Processor Cache: 2 mb; Processor Speed: 3 Ghz; Memory: 8 GB DDR4 Expandable; Storage: 256 GB SSD Expandable; Power Supply: 220 V; Network Controller: Ethernet and Wireless Support; Ports: HDMI, USB Ports – 3; Battery Life: Minimum 5 hours; and Display: 13 - 17 Inch.

UG_DHS_CI01_02_Rt1_IS3: ***PDA/IPAD/TAB*** - Processor Speed: 2 Ghz; Memory: 4 GB; Storage: 32 GB; Display: 10 inch tablet; Camera Min: 2 MP; Battery Life: Minimum 5 Hours; Ruggedness: Min Drop height 70 cm; and Connectivity: Mobile data support, Mi 4G/LTE/GSM Connectivity, Wifi, Hotspot; SIM: Nano-SIM; DISPLAY Type: TFT capacitive touchscreen, 16M colours; Bluetooth: 5.0, A2DP, LE GPS: Yes, with A-GPS, GLONASS, GALILEO, BDS USB: 2.0, Type-C 1.0 reversible connector FEATURES: Sensors Accelerometer, gyro, compass.

UG_DHS_CI01_02_Rt1_IS4: Local **d**ata backup medium should be sufficient to meet the health facility needs

(i). National Referral Hospitals……10Tb
(ii). Regional Referral Hospitals …....5Tb
(iii). General Hospitals ……..2Tb
(iv). HC IV & III ……..…..1Tb

UG_DHS_CI01_02_Rt1_IS5: **Biometric Fingerprint Reader-** Connection: USB 2.0; Operating System's: Microsoft Windows (32-bit and 64-bit), Linux (32-bit and 64-bit), Android; Resolution: 512 ppi; Image capture area (Platen size): 15 x 18 mm (0.6″ x 0.7″); Sensor type: Optical; Illumination: Blue LEDs; Device size: 65 x 36 x 16 mm (2.6″ x 1.4″ x 0.6″); Operating temperature: 0°C ~ +40°C; Operating humidity: 20-80 (non-condensing).

UG_DHS_CI01_02_Rt1_IS6: **Raspberry Pi** – Processor Speed: 2 Ghz; Memory: 8 GB DDR4; Storage: 128 GB; SSD Expandable Display: 17-inch LED Monitor; HDMI & VGA Ports; Case for Raspberry Pi 4 with Fan, Vesa Mount, USB Keyboard, USB Mouse.

UG_DHS_CI01_02_Rt1_IS7: **Other ICT Devices-**Printers, Scanners and Photocopiers should be fast with high-resolution prints/scans. They should all support high-quality resolution of at least 200 DPI.

UG_DHS_CI01_02_Rt2: Software running on the devices should be licensed and support installation (be compatible) of other DH applications.

Implementation Specification(s)

UG_DHS_CI01_02_Rt2_IS1: Min OS & Runtime environment -Microsoft OS: Windows 8.1 classic & later or macOS 10.14 (Mojave); Web Browser: Microsoft Internet Explorer 11 & later, Microsoft Edge or Safari 12, Google Chrome of 2010 and above, Mozila Firefox 4 and above.

Java Runtime Environment (JRE): Oracle JRE 8 up to 8u231. For macOS, JRE 8 or later versions for the smart card reader.

UG- DHS_CI01_03: Minimise diverse implementation of the DHCI

Statement

Reduce diversity of DHCI implementations that support healthcare programmes and interventions through procurement and implementation based on contextualised global standards and minimum specifications laid down by MoH and related MDAs.

Rationale

UG- DHS_CI01_03_*Rt1*: The MoH enforces implementation and use of interoperable DHCI and applications capable of facilitating exchange of health data/information across all health system levels.

Implementation Specification(s)

UG- DHS_CI01_03_*Rt1_IS1:* Adopt and use ANSI/TIA-1179 - A standard for health communication infrastructure to support best practices in the design and implementation of the DHCI that facilitate intra- / inter-facility exchange.

UG- DHS_CI01_03_*Rt1_IS2:* ICT devices used for handling DH data should be housed in an environment that meets the requirements of a Tier 2 data centre (TIA-942 Telecommunications Infrastructure Standard for Data Centres[1]), including;

(i). Cooling and Temperature: Ambient room temperature of 15-32 degree Celsius; Fire detection and Suppression;

(ii). Physical Security: Two Factor authentication for access e.g., (Pin and biometric fingerprint); Secure door; Surveillance with Intrusion detection; and Fire detection and Suppression

(iii). Power supply and Backup: 48 hours backup time (Time to recover from an incident on main power supply); and Clean uninterrupted power supply.

2.2.2. COMMUNICATION NETWORKS & CONNECTIVITY STANDARDS

UG_DHS_CI01_04: Standardised Connected Health Systems

Statement

Healthcare facilities/ organisations participating in the connected health system should establish DH communication network(s) with quality devices, data rate, & suitable network services to support secure HIE.

[1] A data centre is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g. air conditioning, fire suppression and security devices)

Rationale

UG_DHS_CI01_04_Rt1: All participating health organisation/ facilities implement DHCI that meet the required hardware, software, network and security specifications for quality health data.

Implementation Specification(s)

UG_DHS_CI01_04_Rt1_IS1: MoH, telecommunication organisations should provide fast and reliable network connectivity to all service delivery points, both LAN and the Internet (that uses the networking protocols: TCP/IP Version 4, VPN, & WLAN-802.11) to ensure a reliable connectivity that support all modes of HIE. We recommend that ANSI/TIA-1179-A be adapted to include clauses stipulating that;

(i) All health service delivery points have procured end-user ICT devices with at least min. specifications as laid down in the "**ICT INFRASTRUCTURE STANDARDS SPECIFICATION DOCUMENT**".

(ii) Communication HW, SW, computer networks, and migration middleware should conform to MoH and related MDAs defined standards to ensure interoperability between systems and devices participating in the connected health system.

(iii) Healthcare sites/healthcare organisations must ensure the reliability and security of the health data/information being exchanged over the communication network. Health data sharing policies and procedures should also ensure infrastructure capability to securely support information sharing.

(iv) Guidelines for DH HW, SW and Communication Network, must be fully documented and made public (identifiable) for all healthcare stakeholders to have a copy that they can follow.

(v) The mechanisms for monitoring compliance of different DH communication network implementation against MoH and related MDA's defined standards should be in place.

UG_DHS_CI01_04_Rt1_IS2: Each entity participating in the connected health system should comply with MoH's minimum specifications for connectivity devices of their health system level.

(i). **Firewall**: CPU Cores: 4 Core; Physical Network I/O ports: (1) 10GB SFP), (4) 1 Gbps RJ-45 "direct" (unswitched) ethernet (LAN)/(WAN); Storage 16 GB - upgradable; Memory: 8 GB DDR4; Console: Port 1 console port; USB Ports: 2x USB 3.0; Mounting: Optional wall mount kit; Functionality features: DNS Server, DHCP Server, Proxy, IDS/IPS, Packet capture / inspection, NAT & PAT, QoS, Software load balancer, Traffic monitoring, Traffic logging, statistics, and graphs, Traffic shaping, VLAN, Wake-on-LAN, and Web filtering.

(ii). **Switches**: (a) Managed switches - Ports: 8/ 16/ 24/ 48; Networking Interfaces: 10/100/1000 Mbps RJ45 Ports AND 1 Gbps SFP Ports; PoE: Output (RJ45 Ports) IEEE 802.3at/af; Operating Temperature: -5 to 45° C (23 to 113° F); Power Method: 100-240VAC/50-60 Hz, Universal Input preferably dual power supply; and Other Considerations include L3 support for 24/ 48 port switches, GUI for configurations to

ease support or Rack Mountable. (b) Unmanaged switches - Ports: 8/ 16/ 24; Networking Interfaces: 10/100/1000 Mbps RJ45 Ports AND 1 Gbps SFP Ports; Operating Temperature: -5 to 45° C (23 to 113° F); Power Method 100-240VAC/50-60 Hz, Universal Input; and Other Considerations include Rack mountable.

(iii). **Access Points**: (a) Indoor Access Points – Wi-Fi Standards: 802.11 a/b/g/n/ac/ac; Networking Interface: RJ45 GbE; Wireless Security: WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3, TKIP/AES); Operating Frequency: 2.4 GHz, 5 GHz; Throughput: 2.4GHz- 300 Mbps, 5GHz- 1733 Mbps; Operating Temperature: -5 to 45° C (23 to 113° F); Power Method: 100-240VAC/50-60 Hz, DC Power adapter, P.O.E; and Other Considerations: Mounting Wall/Ceiling, Mesh capability, 50 users. (b) Outdoor Access Point – Wi-Fi Standards: 802.11 a/b/g/n/ac/ac; Networking Interface: (1) RJ45 GbE; Wireless Security: WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3, TKIP/AES); Operating Frequency: 2.4 GHz, 5 GHz; Throughput: 2.4GHz- 300 Mbps, 5GHz- 1733 Mbps; Operating Temperature: -5 to 45° C (23 to 113° F); Power Method: 100-240VAC/50-60 Hz, DC Power adapter, P.O.E; and Other Considerations including Mounting Wall/Ceiling, Mesh capability, Water and dust resistant, 50 users.

(iv). Server Specifications and Rack: (a) Regional Referral Hospital – Rack Size: 42 U; Processor family: Xeon; No. of Processors: 1 or 2; Cores: 8; Processor Cache: 8 mb; Processor Speed: 3 Ghz; Power Supply: 2 flexible power supplies; Memory: 64 GB DDR4; Storage: 1 TB x 4 Disks - Raid configurable; Network Controller: 1GBps, 4ports Ethernet, 2 SFP+ 10 GBps ports; Rackmount Console with KVM Switch: 19 inch display, LED back lit, Touchpad and keyboard, VGA and HDMI support, USB ports; and Other Considerations include Rack Mountable with rail kit, Warranty 3 years, Windows Server 2019 licence, PDU. (b) General Hospital - Rack Size: 25 U; Processor family: Xeon; No. of Processors: 1 or 2; Cores: 8; Processor Cache: 8 mb; Processor Speed: 3 Ghz; Power Supply: 2 flexible power supplies; Memory: 32 GB DDR4; Storage: 1 TB x 2 Disks - Raid configurable; Network Controller: 1 GBps, 4 ports Ethernet, 2 SFP+ 10 GBps ports; Rackmount Console with KVM Switch: 19 inch display, LED back lit, Touchpad and keyboard, VGA, HDMI support, USB ports; and Other considerations such as Rack Mountable with rail kit, Warranty 3 years, Windows Server 2019 licence, PDU. (c) Health Centr IV – Rack Size: 15 U; Processor family: Xeon; Cores: 2; Processor Cache: 2 mb; Processor Speed: 3 Ghz; Memory: 16 GB DDR4; Storage: 1 TB; Network Controller: 2 ports Ethernet; Display: 19-inch display, LED back lit, Mouse and keyboard, VGA, HDMI support, USB ports; and other considerations like the Microserver size, Warranty of atleast 3 years, Windows Server 2019 licence, and PDU. (d) Health Centre III – Rack Size: 15 U; Processor family: i7; Cores: 2; Processor Cache: 2 mb; Processor Speed: 3 Ghz; Memory: 16 GB DDR4; Storage: 1 TB; Network Controller: Ethernet; Display, KVM: 19-inch display, LED back lit, Mouse and keyboard, VGA, HDMI support, USB ports; and other considerations like Microserver size, at least a warranty 3 years, Windows Server 2019 licence, and PDU.

UG_DHS_CI01_04_Rt1_IS3: All participating healthcare organisations implement data communication networks and infrastructure that support QoS, Security and Privacy.

(i). Implementations of guided networking/transmission media should be based on Cat3 and higher, and Fiber Optic (preferred because of higher data rate and security).

(ii). Healthcare cites /devices and networks should support VPN and TCP/IP networking protocols and emerging Bring Your Own Device (BYOD).

(iii). The wireless LAN should follow the 802.11 protocol suite.

(iv). Healthcare sites should be connected to MoH designated Cloud Service(s) and Data Centre(s).

UG- DHS_CI02_01: MoU Specifying Telecom and Internet service Provision

Statement

Any form of MoU and SLA (as part of the social corporate responsibility) between telecom and Internet service providers should specify both quality and terms of service provision to Uganda's health sector.

Rationale

UG- DHS_CI02_01_Rt1: There is reliable and affordable (subsidised) connectivity to support all forms of HIE in healthcare.

Implementation Specifications

UG- DHS_CI02_01_Rt1_IS1: An MoU is established between MoH and Telecom/Internet Service Providers (ISPs) stipulating the quality and conditions for Internet services to be provided to support healthcare interventions in Uganda.

UG- DHS_CI02_01_Rt1_ *IS2:* The MoU with telecom and Internet service providers should specify and establish a mechanism for monitoring QoS for health programs in Uganda.

UG- DHS_CI02_01_Rt1_ *IS3:* *Other Arrangements.* The MoH and related MDAs have structures and a mechanism for monitoring QoS provided by Internet service providers who have agreements to connect healthcare service delivery points.

UG- DHS_CI02_02: Last Mile Connectivity

Statement

NITA-U should connect all health facilities to the National Backbone Infrastructure.

Rationale

UG- DHS_CI02_02_Rt1: Government Health facilities and Service delivery points are connected to the National Data Transmission Backbone Infrastructure.

Implementation Specifications(s)

UG- DHS_CI02_02_Rt1_IS1: MoH should determine and prioritise connectivity needs for all healthcare sites in Uganda

UG- DHS_CI02_02_Rt1_IS2: NITA-U should follow the MoH priority list for connecting healthcare facilities and service delivery points to the national Backbone.

2.2.3. APPLICATION, SOFTWARE AND TECHNOLOGIES STANDARDS

UG_ DHA_IM03_01: Application Design & Development

Statement

DH application designing and development is guided by agreed standards and guidelines as contextualised by MoH and related MDAs, which specify modes for linking (sharing) health data between applications in a secure manner.

Rationale

UG_ DHA_IM03_01_Rt1: Design, development, and deployment of DH applications are guided by standards that specify modes for linking (sharing) health data from across DH applications in a secure manner.

***Implementation Specification*(s)**

UG_ DHA_IM03_01_Rt1_IS1: MoH should develop and enforce guidelines and standards required for the development and use of standardised DH applications.

UG_ DHA_IM03_01_Rt1_IS2: Development of DH applications should demonstrate alignment with approved/contemporary software development life cycle.

UG_ DHA_IM03_01_Rt1_IS3: The application interface design and features are consistent across all DH applications being adopted/developed for use in healthcare interventions/programs in Uganda.

UG_ DHA_IM03_01_Rt1_IS4: DH applications should follow data interoperability standards

UG_ DHA_IM03_02: Mandate to Oversee all DHCI Implementation

Statement

MoH superintends the implementation and use of DH applications in public and private healthcare sites.

Rationale

UG_ DHA_IM03_02_Rt1: The MoH has mechanisms for regulating development and deployment of DH applications for healthcare services in Uganda.

Implementation Specification(s)

UG_ DHA_IM03_02_Rt1_IS1: MoH directs the acquisition of all DH applications and or owns them after rigorous testing and approval for use in the health sector.

(i). The MoH tests, approves and maintains a database of all DH applications in the country

(ii). The MoH, where possible, should own or be a party to the Intellectual Property Rights (IPR).

(iii). The applications and or software may be supplied or availed by government or commercially

UG_ DHA_IM03_02_Rt2: MoH superintends DH infrastructure/ Applications implementation and use at both public and private health facilities.

Implementation Specification(s)

UG_ DHA_IM03_02_Rt12_IS1: The MoH ensures that an agreement addressing detailed protocols for data collection, transmission, processing, storage and use is signed between all healthcare sites/organisations involved.

UG_ DHA_IM03_02_Rt2_IS2: MoH supervises the implementation of guidelines on use of the DH applications and data that they hold.

UG_ DHA_IM03_04: Acceptable DH Technologies

Statement

Control choice of DH technologies to be adopted and used by healthcare organisations, facilities and researchers to ensure interoperable and secure collection, sharing and use of health data/information.

Rationale

UG_ DHS_IM03_04_Rt1: MoH should determine and enlist acceptable (including emerging) ICT technologies that healthcare participating entities can adopt to support healthcare processes in Uganda.

Implementation Specification(s)

UG_ DHS_IM03_04_Rt1_IS1: The MoH has a database of approved and listed ICT technologies that can be used in the country. Example of such technologies are;

(i). Internet of Things (IoT) which is a collection of devices, services and software that integrates data received from various connected devices for patient monitoring or health management e.g., Body area Networks

(ii). Big data technologies

(iii). mHealth, Telemedicine, etc

(iv). Blockchain technologies

UG_ DHS_IM03_04_Rt1_IS2: MoH has criteria for evaluating implementations of these technologies. The evaluation criteria should support scoring for continued use or decommissioning of such ICT technologies in Uganda's health system.

UG_ DHS_IM03_04_Rt1_IS2: The MoH has a safe migration policy and procedure for decommissioning the technologies once they have been considered outdated/inappropriate for Uganda's healthcare environment.

2.2.4. DHCI's FACILITATING RESOURCES STANDARDS

UG_ DHC_IT01_01: *Training of DH Users*

Statement

The MoH, collaborating medical training institutions and the DH implementing partners should aim at producing an all-rounded, knowledgeable and skilled digital health workforce capable of observing stipulated guidelines.

Rationale

UG_ DHC_IT01_01_Rt1: Ensure all rounded, knowledgeable and skilled DH health workforce for improved service delivery.

Implementation Specification(s)

UG_ DHC_IT01_01_Rt1_IS1: Training institutions have revised/updated/developed their curricula with courses aimed to produce all-rounded DH with expertise in using DH applications and supporting CI.

UG_ DHC_IT01_01_Rt1_IS2: DH workers are trained to use existing DH applications and support CI under strict observance of health data/information security and privacy guidelines.

UG_ DHC_IT01_01_Rt1_IS3: The MoH should stipulate the required minimum DH competencies for the different digital health workforce/roles.

UG_ DHC_IT01_01_Rt1_IS4: Incorporate the basic criteria of DH competency into recruitment material and processes to help attract and hire healthcare workers with the appropriate educational background and experience to use the DH technologies.

UG_ DHC_IT01_01_Rt1_5: Develop a competency assessment tool or skills assessment based on the Competency Framework or another benchmark. The competency assessment tool can be used to complete a periodic skills assessment of the health workers' activity to identify gaps (training needs assessment).

UG_ DHC_IT02_01: Training of Managers responsible for DHCI

Statement

Leaders/managers responsible for DHCI are informed and trained on the use of DH technologies and trends.

Rationale

UG_ DHC_IT02_01_Rt1: Leaders/managers responsible for DHCI are made aware of emerging technologies and trends to support their decision-making process.

Implementation Specification(s)

UG_ DHC_IT02_01_Rt1_IS1: MoH has developed mechanisms for identifying and documentation of relevant emerging DH technologies and trends.

UG_ DHC_IT02_01_Rt1_IS2: Leaders/managers responsible for DHCI are made aware and trained to use DH technologies to support their tactical and strategic decision making.

(i). Managers responsible for DHCI are made aware of emerging DH technologies and trends that have been identified.

(ii). Managers/leaders responsible for DHCI have the skills and knowledge required to use DH technologies in decision-making and planning.

UG_ DHS_CI03_01: *DHCI Financing*

Statement

Adequate funds should be allocated to finance the DHCI that supports DH data collection, processing and information sharing in Uganda.

Rationale

UG_ DHS_CI03_01_Rt1: Resources are identified and equitably allocated to the critical areas of the DHCI for efficient deployment of DH in a manner that enables the health sector levels (National & Subnational) acquire and implement the DHCI defined for the different levels by MoH.

Implementation Specification(s)

UG_ DHS_CI03_01_Rt1_IS1: MoH should identify financial resources, including sources of funds and ensure equitable allocation to the critical areas of the DHCI.

UG_ DHS_CI03_01_Rt1_IS2: MoH should ensure acquisition and implementation of DHCI to the different health service delivery points as defined for their levels.

UG_ DHS_CI04_01: *Reliable Electric Power Supply*

Statement

Reliable and alternative sources of electric energy are available at all healthcare service delivery points.

Rationale

UG_ DHS_CI04_01_Rt1: Whenever possible, DH systems are powered by electric connections to the national grid and or alternative smart sources of electric energy are made available at all health service delivery points.

***Implementation Specification*(s)**

UG_ DHS_CI04_01_Rt1_IS1: The MoH and related MDAs are required to support the electrification programme of connecting all health facilities to the national power grid.

(i). MoH should engage relevant MDAs responsible for the electrification programme through provision of documentation of priority health facilities requiring connection to the national grid.
(ii). Relevant MDAs should support connection of priority health facilities to the national grid.

UG_ DHS_CI04_01_Rt1_IS2: MoH and related MDAs are required to define and provide (when possible) suitable alternative sources of clean energy to health facilities and community level service delivery points (whether government, for-profit or not-for-profit healthcare institutions) to power the DH systems to ensure their reliability.

2.2.5. SECURITY AND PRIVACY STANDARDS

UG_ DHS_SP02_01: ***DH Information Security Access Rights***

Statement

DH information security access rights are properly assigned and managed.

Rationale

UG_ DHS_SP02_01_Rt1: Appropriate information access and security clearance levels are assigned (based on the relevancy of their roles or duties) and managed for all members of the workforce and other authorised parties.

Implementation Specification(s)

UG_ DHS_SP02_01_Rt1_IS1: Designate a person responsible for overseeing adherence to security policies and procedures as required by the standard for all participating entities or associates.

UG_ DHS_SP02_01_Rt1_IS2: Regardless of medium, consistently apply and enforce levels of information protection throughout the DH device, technology or network lifetime.

UG_ DHS_SP02_01_Rt1_IS3: The DHCI data / information security processes should be aligned to national and international security guidelines.

UG_ DHS_SP02_01_Rt1_IS4: Applicable security controls should be put in place to protect electronic data that is resident on DH devices.

UG_DHS_SP02_01_Rt1_IS5: Proper security measures are implemented and strictly enforced for the DH Applications/ISs that manage electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

UG_DHS_SP02_01_Rt1_IS6: Information access management procedures are implemented for authorising access to electronically protected health information that are consistent with assigned access rights.

UG_ DHS_SP02_02: ***DH Data/Information Transmission Security***

Statement

Develop policy-based guidelines for securing the DH data/information transmission.

Rationale

UG_ DHS_SP02_02_Rt1: The MoH and related MDAs responsible for the DH standardisation have developed guidelines for data/information transmission within and between networks and devices.

Implementation Specification(s)

UG_ DHS_SP02_02_Rt1_IS1: There should be proper guidelines and documentation for approving ICT devices to be used on the DHCI network.

UG_ DHS_SP02_02_Rt1_IS2: The MoH and related MDAs responsible for the DH standardisation review security and access requirements and consequently revise them annually.

UG_ DHS_SP02_02_Rt1_IS3: Security requirements should ensure that any third-party user of the personal protected information like a health insurance company must ensure reasonable and appropriate safeguard for electronic data under their custody.

UG_ DHS_SP02_02_Rt1_IS4: Technical security measures are implemented to guard against unauthorised access to electronic protected health information that is being transmitted over an electronic communications network.

UG_ DHS_SP02_03: *Data Protection – Confidentiality and Integrity*

Statement

Enforce measures that provide for data/information confidentiality and protection are implemented and enforced across the entire health sector.

Rationale

UG_ DHS_SP02_03_Rt1: The MoH and participating entities in the health sector ensure protection and privacy of personally identifiable data that the DHCI contains.

Implementation Specification(s)

UG_ DHS_SP02_03_Rt1_IS1: Measures that provide confidentiality and integrity of health data/information are implemented and enforced across the entire health sector.

(i). Policies and procedures are implemented to protect electronic health information from improper alteration or destruction.

(ii). Ensure confidentiality of personally identifiable data and information at all stages of the HIE.

(iii). DH users should strictly adhere to data protection, and privacy laws and guidelines regarding electronic data collection, processing, retention, and exchange.

UG_ DHS_SP02_03_Rt1_IS2: *Person or entity authentication, Audit controls:* DH systems have M&E and Audit concerning security and privacy risks faced by health data residing on them and how they can be mitigated.

(i). There are mechanisms to authenticate all nodes and keep an audit trail of all system transactions.

UG_ DHS_SP02_04: Improve user observance of security and privacy guidelines

Statement

Users are conversant and comply with DHCI relevant security and privacy laws, and guidelines including Uganda's Data Protection and Privacy Act regarding electronic data collection, processing, retention, and exchange.

Rationale

UG_ DHS_SP02_04_Rt1: There is widespread sensitisation and monitoring to improve user compliance with DHCI relevant security and privacy laws, standards/guidelines.

Implementation Specification(s)

UG_ DHS_SP02_04_Rt1_IS1: Users should be sensitised about existing relevant DHCI security and privacy laws, standards/ guidelines.

(i). DH User compliance with relevant DHCI security and privacy standards/ guidelines is improved through wide sensitization and compliance monitoring.

UG_ DHS_SP02_04_Rt1_IS2: Users observe all relevant DHCI security and privacy laws and guidelines.

UG_ DHS_SP02_04_Rt1_IS3: The MoH shall avail DH implementers and users with proper documentation of security and privacy laws, standards / guidelines including Uganda's Data Protection and Privacy Act.

UG_ DHS_SP02_05: *Mitigation of security risks*

Statement

DH systems have mitigation plans addressing security risks faced by DHCI and the health data they contain.

Rationale

UG_DHS_SP02_05_Rt1: All entities in the health sector must mitigate, to the extent practicable, any harmful effect that may result from the violation of security policies and guidelines or the requirements.

Implementation Specification(s)

UG_DHS_SP02_05_Rt1_IS1: All entities in the health sector should actively participate in the identification, documentation and reporting of possible security risks to the DHCI.

UG_DHS_SP02_05_Rt1_IS2: There are well documented DHCI mitigation plans and mechanisms to handle security/privacy risks identified, documented and reported.

UG_DHS_SP02_05_Rt1_IS3: MoH has a program for periodic technical and nontechnical verification/evaluation of the DHCI security measures to ensure that the security safeguards are effectively implemented and that the safeguards are continually updated in response to new risks or deficiencies.

UG_DHS_SP02_05_Rt1_IS4: A contingency plan is developed and implemented to respond to any emergency or other occurrences like fire, vandalism, system failure, and natural disaster that damages systems that contain health data/information.

SECTION 3: DH WORKFORCE CAPACITY BUILDING FRAMEWORK

A digital health worker (DHW) is a health worker with capabilities to use digital devices, applications and or systems. A DH competency model with corresponding set of standards for human resources development and training regards DH competencies is provided to facilitate health workers to become digitally competent in their work-practices.

DH COMPETENCY MODEL

The competency model provides proficiency levels required for the different health work knowledge domains, and Uganda's DHW job roles and required proficiencies. Focus of the assessment criteria aims to train a DHW with the attributes defined in the DH curriculum for the African region, i.e., communicator, a collaborator, a professional, an advocate and a manager; data analyst, and technology expert (Alunyu et al., 2020).

DHW JOB ROLES AND REQUIRED PROFICIENCIES

A DHW can include all individuals working in healthcare/third party health organisations providing healthcare, health facilities, or even in communities (CHWs) who use ICT to provide health services. Depending on their roles and responsibilities in the health sector, these persons require differing levels of knowledge and/or skills to use ICT in health to develop guidelines, standards or policy and promote use of ICT in health, make decisions regarding deployment, and/or use ICT in the health environment. The DHW domains for training include soft skills, digital health knowledge and use skills, information technology (IT) technical skills, enterprise architecture skills, program or project management skills, and legal environment.

(i). **DH policy and regulation management**: this role entails leading the development, implementation and maintenance of DH policy, standards, guidelines, and all manner of regulations in the DH space. Some of the job positions include health policy makers, DH policy advisors, standards specialists, etc.

(ii). **DH managers/leaders**: this includes persons in the position of authority, who oversee the implementation and use of DH. Examples include health facility administrators, heads of departments, directors, commissioners, etc.

(iii). **DH technical managers/architects**: this role includes different facets of DH including enterprise architecture, data management, IT infrastructure, Software and Application Development/Management, DH Security and privacy, etc.

(iv). **DH application and technology users**: Any HW who uses ICT to support their work routines.

PROFICIENCY LEVELS REQUIRED FOR DIGITAL HEALTH WORKER (DHW) IN UGANDA

Table 21 shows Four proficiency levels that are recommended for DHWs in Uganda, i.e., Basic level=1, Intermediate=2, Advanced=3, and Expert=4. Knowledge/skill domains where a health worker does not require proficiency shall be scored a zero (0) value.

Table 21. Proficiency Levels of DHWs (adopted from Alunyu et al., 2020)

Level of proficiency	Level 1 – Basic	Level 2 – Intermediate	Level 3 - Advanced	Level 4 - Expert
Brief description	This is foundational & develops the DHW's literacy level. Provides common knowledge or understanding of basic DH technology techniques and concepts e.g., types of technology, what for, how to use, etc. Key terms are use, find, identify, etc.	Training at this level aims at developing the DHW capability to independently use DH technology to complete tasks and to apply DH technology knowledge or skill in different situations. Key terms include explain, describe, illustrate, among others	Advanced training equips the DHW with techniques to apply theory. Can perform DH technology tasks without help, it's a level of DH technology professionalism. Key terms are apply, show, propose, explain, vary, assess, etc.	This level prepares a DHW to provide guidance on specific DH technology(ies), troubleshoot and answer questions related to them or an area of expertise within the technology. The DHW becomes the consultant – "go to person" Key terms include create, integrate, propose, etc.
Expected Outcomes	i. Understand and can identify medical / DH terminologies, concepts, principles, and issues ii. Can utilize a full range of DH technologies	i. Occasionally apply knowledge to different cases with minimal guidance ii. Understand and can discuss the application and implications of DH technology changes to processes, policies, and procedures iii. Chooses appropriate tools for tasks iv. Experiments with new processes, tools, or technologies to determine the applicability	i. Provide practical/relevant ideas and perspectives on DH technology processes or practice improvements to be implemented ii. Coach others in the application DH technologies translating complex problems to solvable forms iii. Support the DH technology development including references and resource materials	i. Demonstrate consistent excellence in applying DH technology expertise across multiple projects and/or health systems ii. Create new technologies/application scenarios iii. Explain the relevant DH technology process elements and issues in relation to organisational issues and trends in sufficient detail
Possible competencies	i. Can use computers & other ICTs ii. Can identify appropriate DH technologies iii. Browse, search, filter data, information, and digital content iv. Distinguish data, information and digital content v. Can understand DH & medical terminologies, identify diseases codes, etc. vi. Can use inbuilt security measures	In addition to level 1 competencies, can; i. Evaluating data, information and digital content ii. Managing data, information and digital content iii. Interact through digital technologies iv. Share through digital technologies v. Engage in citizenship through digital technologies vi. Collaborate through digital technologies vii. Netiquette viii. Managing digital identity	In addition to level 2 competencies, level 3 DHW can; i. Develop DH content ii. Integrate and re-elaborate on the DH digital content iii. Solve technical but DH related problems iv. Shares expertise, teaching skills and explaining concepts to others v. Copyright and licenses	In addition to level 3 competencies, level 4 DHW can; i. Improves or redesigns DH processes, tools or technology ii. Implement and troubleshoot complex issues on DH technology(ies) of their expertise iii. Programming
Possible competency categories	i. Technology literacy & usage skills ii. Literacy in medical & DH terminologies iii. Information & data Literacy iv. Security & privacy Literacy	In addition to level 1 competency categories are; i. Digital communication ii. DH products & services	In addition to level 2 categorization; i. Regulation & compliance (implementation) ii. Business processes	In addition to level 2 categorization; i. Networking and Programming ii. Data analytics
Example of security & Privacy application	SECURITY and PRIVACY (Required at all levels of competency to protect devices, personal data, health & wellbeing and environment)			
	Protect devices, use security measures on devices & inside applications, etc.;	Protect devices, use security measures on devices, inside applications, on data/ information sharing, etc.	Protect & guide others on how to protect devices, applications, data/ information privacy, etc.	Improve or develop systems to enforce security & privacy

CONCLUSION

Notwithstanding numerous benefits that can be realised from implementing Digital Health (DH) in Uganda's health system, lack of standardisation and non-interoperability have caused most DH interventions to remain isolated and uncoordinated; hence affecting data use and utilisation in healthcare and service delivery, decision-making and informing policy. This Guide fills the gap by detailing what is needed to standardise Digital Health in Uganda's health system. Particularly, the Standardisation Guide provides a comprehensive set of Digital Health Enterprise Architecture, Standards and Knowledge products (DH-ASK) guidelines, that if implemented as prescribed, can facilitate a sustainable Digital Health environment for Uganda's health system. Additionally, if standards for DH capacity building are implemented as prescribed, these can aid production of competent DH practitioners that are able to; lead DH policy development, management and regulation; develop, implement and maintain DH systems; and proficiently use the deployed DH systems in Uganda. As such, supporting realisation of MoH's mission to provide the highest possible level of health services to all people in Uganda. MoH's next steps include among others; phased implementation and rollout of the DH-ASK Standardisation Guidelines in Uganda's health system, and effective monitoring and evaluation of the DH implementations in the country.

REFERENCES

Adebesin, F., & Kotzé, P. (2017). A process for developing an e-health standards selection method artefact using design science research. *Journal of Design Research*, *15*(3–4), 258–287.

Adebesin, F., Kotze, P., Foster, R., & Van Greunen, D. (2013). A Review of Interoperability Standards in E-health and Imperatives for their Adoption in Africa. *South African Computer Journal*, *50*(1), 55–72.

Alunyu, A. E., Munene, D., & Nabukenya, J. (2020). Towards a Digital Health Curriculum for Health Workforce for the African Region: A Scoping Review. *Journal of Health Informatics in Africa*, *7*(1), 38–54.

Alunyu, A. E., & Nabukenya, J. (2018). *A Conceptual Model for Adaptation of eHealth Standards by Low and Middle-Income Countries*. *5*(2), 10–16. https://doi.org/10.12856/JHIA-2018-v5-i2-199

Alunyu, A. E., Wamema, J., Kiwanuka, A., Moses, B., Amiyo, M., Kambugu, A., & Nabukenya, J. (2021). *Investigating the impediments to accessing reliable, timely and integrated electronic patient data in healthcare sites in Uganda*.

ANSI/BICSI, & Institute, A. N. S. (2018). *Information Communication Technology Systems Design and Implementation Best Practices for Healthcare Institutions and Facilities: ANSI/BICSI 004-2018*. BICSI. https://books.google.co.ug/books?id=6GjYvQEACAAJ

Ashaba, J., & Nabukenya, J. (2022). Beyond monitoring functionality to results evaluation of eHealth interventions: Development and validation of an eHealth evaluation framework. *Health Informatics Journal*, *28*(4), 1–16. https://doi.org/10.1177/14604582221141834

Barateiro, J., Antunes, G., & Borbinha, J. (2012). Manage risks through the enterprise architecture. *2012 45th Hawaii International Conference on System Sciences*, 3297–3306.

Costello, M., & Parker, J. (2020). *Related Documents 1. A Health Interoperability Standards Development, Maintenance and Management Model for Australia, Executive Summary Report, Final, Version 1.0, 30 June 2019. 2. A Health Interoperability Standards Development, Maintenance and Management* (p. 145). http://www.jpconsulting.com.au

Council of the European Union. (2004). *List of standards and/or specifications for electronic communications networks, services and associated facilities and services* (p. 144). https://www.etsi.org/deliver/etsi_sr/002200_002299/002211/01.01.01_60/sr_002211v010101p.pdf

European Parliament. (n.d.). *eHealth – Technology for health—Think Tank*. Retrieved 27 November 2017, from http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)551324

European Union. (2015). *eHealth Network: Refined eHealth European Interoperability Framework* (p. 24). https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf

European Union. (2019). *eHealth Network Guidelines* (p. 22). https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co922_en.pdf

Gary, D., Mark, J., Don, M., John, R., & Helen, S.-L. (n.d.). *ISO/HL7 10781—Electronic Health Record System Functional Mode*.

GoU. (2021a). *E-Government Interoperability Framework Reference Architecture*.

GoU. (2021b). *Government of Uganda e-Government Web Application Security Architecture Framework*.

Hammond, W. E. (2017). Standards for Global Health Information Systems. *Global Health Informatics: How Information Technology Can Change Our Lives in a Globalized World*, 94–108.

Harris, S., & Maymi, F. (2019). *All-in-One CISSP® All-in-One Exam Guide*.

HHS Office of Civil Rights. (2013). *HIPAA Administrative Simplification*.

HIPAA. (2013, August 12). *HIPAA Security Rule Standards and Implementation Specifications.* HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Hudson, B., Hunter, D., & Peckham, S. (2019). Policy failure and the policy-implementation gap: Can policy support programs help? *Policy Design and Practice*, *2*(1), 1–14. https://doi.org/10.1080/25741292.2018.1540378

ISO. (n.d.). *Publicly Available Standards.* Retrieved 23 January 2019, from https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

ISO. (2017). *Health informatics Standards.* https://www.iso.org/committee/54960/x/catalogue/

ISO/HL7. (n.d.). *ISO/HL7 10781:2015 Health Informatics—HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM).* ISO. Retrieved 14 April 2022, from https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/77/57757.html

ISO/IEC. (2018). INTERNATIONAL STANDARD ISO / IEC Information technology—Security techniques—Information security management systems—Overview and. In *ACM Workshop on Formal Methods in Security Engineering. Washington, DC, USA* (Vol. 34, Issue 19).

ISO/IEC. (2019). *Guide 59 ISO and IEC recommended practices for standardization by national bodies. 2019.*

ISO/IEEE. (n.d.). *Novel ISO/IEEE 11073 Standards for Personal Telehealth Systems Interoperability—IEEE Conference Publication.* Retrieved 31 December 2018, from https://ieeexplore.ieee.org/abstract/document/4438177

ISO/TR. (2009). *ISO/TR 11636:2009; Health Informatics—Dynamic on-demand virtual private network for health information infrastructure.* ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/06/50638.html

ITI Planning Committee. (2015). *Health IT Standards for Health Information Management Practices (HIT Standards for HIM Practices).*

ITU-T. (2015). *Recommendation ITU-T H.813: Interoperability design guidelines for personal health systems: Health record network (HRN) interface.*

Josey, A., Harrison, R., Homan, P., Rouse, M. F., Sante, T. Van, Turner, M., & Merwe, P. van. (2018). *The TOGAF® Standard, Version 9.2: A pocket guide* (Issue April). The Open Group.

Kim, T. Y., & Matney, S. A. (2018). Informatics-Related Standards and Standards-Setting Organizations. In *Health Informatics: An Interprofessional Approach* (2nd Edition). Elsevier Inc.

Kiwanuka, A., Bagyendera, M., Wamema, J., Alunyu, A., Amiyo, M., Kambugu, A., & Nabukenya, J. (2021). *Establishing the State of Practice about Data Standards in Monitoring Healthcare Interventions for HIV in Uganda's EMR-based Health Information Systems.* 200–211. https://doi.org/10.5220/0010264302000211

Kotusev, S. (2019). Enterprise architecture and enterprise architecture artifacts: Questioning the old concept in light of new findings. *Journal of Information Technology*, *34*(2), 102–128.

Lau, F., & Kuziemsky, C. (2016). *Handbook of eHealth evaluation: An evidence-based approach.*

Ministry of Health-Uganda. (2010). *The Second National Health Policy 2010/11 to 2019/20.* 30.

Ministry of ICT-Uganda. (2019). *Data Protection and Privacy Act, 2019.*

MoH-Uganda. (2016). *Uganda National eHealth Policy and Strategy.*

MoH-Uganda. (2021). *Strengthening Uganda's Health System through Standardizing Digital Health: Requirements for Digital Health Standards and Enterprise Architecture Framework* (1st ed.). http://library.health.go.ug/health-information-systems/digital-health/strengthening-ugandas-health-system-through-standardizing

NEHTA. (2012). *Standards-Australia.* http://www.e-health.standards.org.au/StandardsOrganisations/NEHTA.aspx

NITA-U. (2010). *ICT Policies, Strategies and Initiatives put in place in Uganda* (p. 12). http://unctad.org/Sections/un_cstd/docs/cstd2010d12_Uganda_en.pdf

NITA-U. (2021). *Uganda e-Government Interoperability Framework (e-GIF).* https://www.nita.go.ug/projects-service-portfolio/uganda-e-government-interoperability-framework-e-gif

Onwubiko, C. (2009). A security audit framework for security management in the enterprise. *Communications in Computer and Information Science*, *45*, 9–17. https://doi.org/10.1007/978-3-642-04062-7_2

PEPfAR. (2019). *The United States President's Emergency Plan for AIDS Relief—United States Department of State.* https://www.state.gov/pepfar/

Singapore Ministry of Health. (2015). *Singapore—National-telemedicine-guidelines-for-singapore.*

The Open Group. (2018a). *The Open Group Architectural Framework Standards* (Version 9.2). https://pubs.opengroup.org/architecture/togaf9-doc/arch/

The Open Group. (2018b). *The Open Group Standard (TOGAF 9.2).*

TR-42.1, T. (2017). *Cabling standard for healthcare facilities_ANSI-TIA-1179-A.*

van de Wetering, R., Kurnia, S., & Kotusev, S. (2021). The Role of Enterprise Architecture for Digital Transformations. *Sustainability*, *13*(4), 2237. https://doi.org/10.3390/su13042237

WHO (2013). *WHO evaluation practice handbook.* World Health Organization.

WHO (2016). *Monitoring and evaluating digital health interventions: A practical guide to conducting research and assessment.*

WHO & ITU. (2012). *National eHealth strategy toolkit.* International Telecommunication Union. http://www.who.int/iris/handle/10665/75211

APPENDICES

APPENDIX A.1 STANDARDISATION FRAMEWORK

Figure 14 illustrates the standardisation framework that can be used to develop standards requirements for Uganda's digital health. It constitutes three major phases (i.e., context setting, standards adaption, and standards implementation).

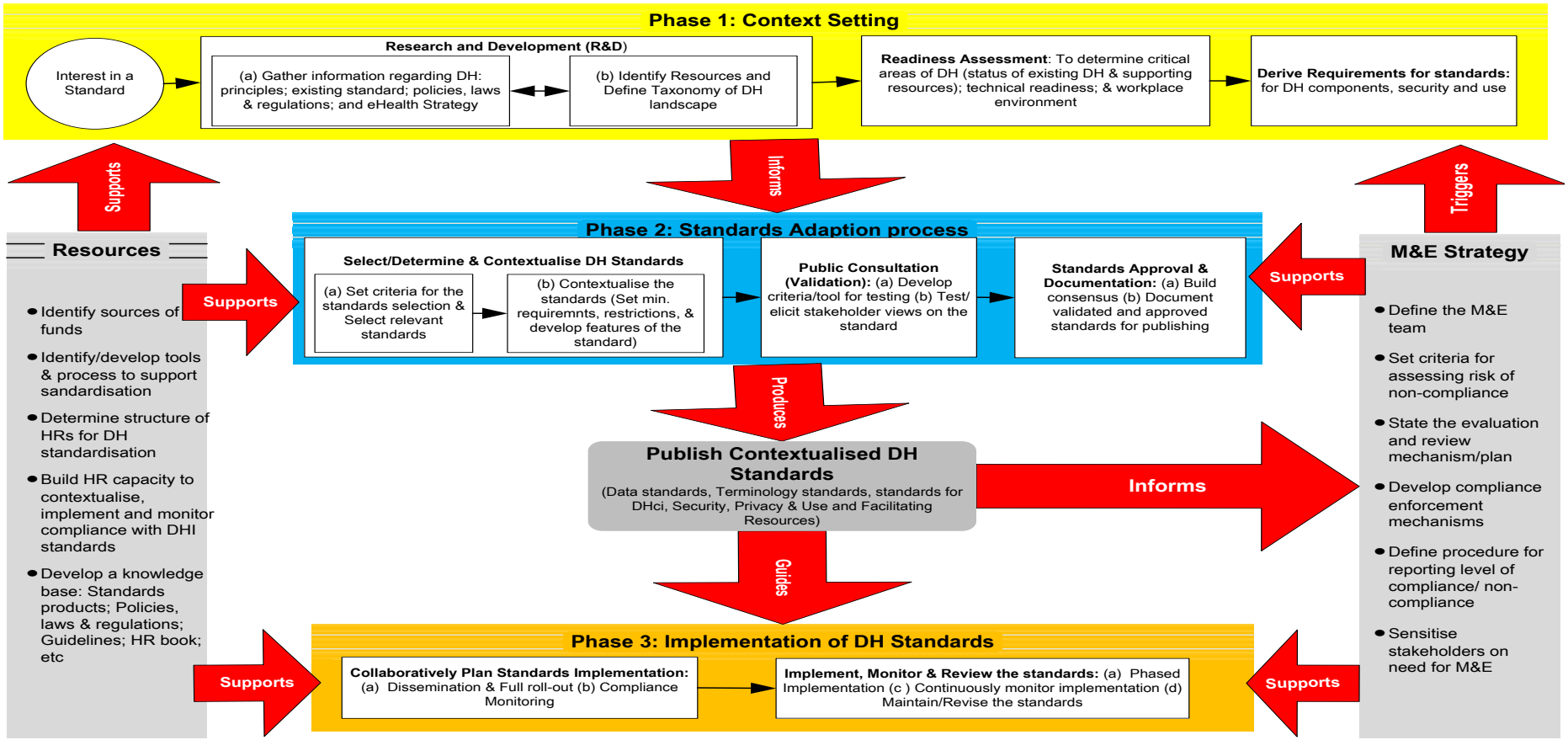


Figure 14. Framework for Standardisation of Uganda's Digital Health Interventions

APPENDIX A.2: STANDARDISATION PROCESS

Error! Reference source not found.**15** illustrates the determination process for filtering suitable Digital Health standards for possible adoption or contextualisation for Uganda's health system.

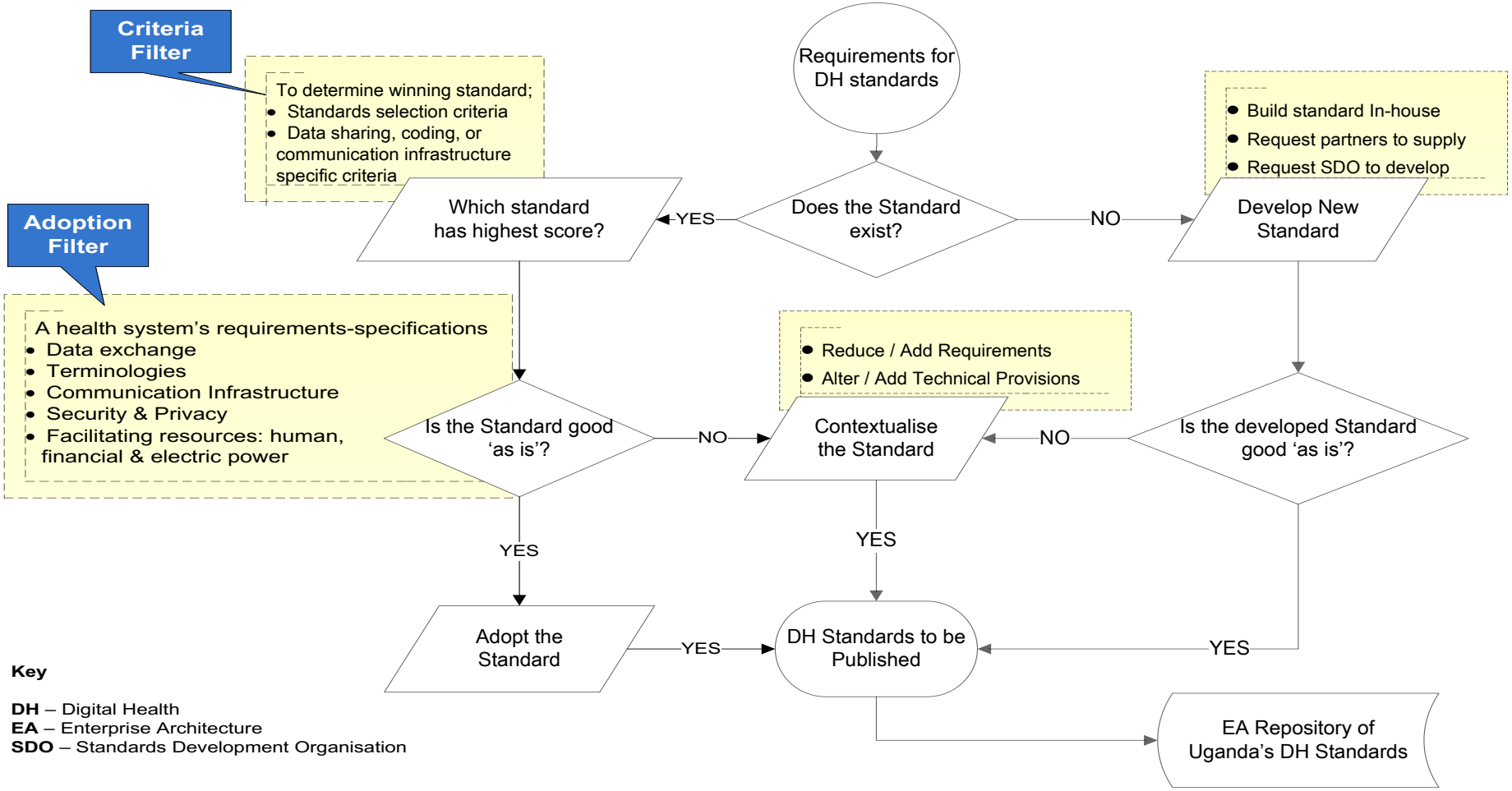


Figure 15. Process of selecting suitable standards for Digital Health

APPENDIX B.1: USE CASE – HIV/TB CLIENT MANAGEMENT SYSTEM ARCHITECTURE FOR IDI CLINIC, MULAGO

The aim of the Digital Health Enterprise Architecture Framework (DHEAF) in Section 1 is to guide the development and implementation of Digital Health Solutions in Uganda. The HIV/TB Client Management System Architecture (HIV/TB CMS) for the Infectious Disease Institute (IDI) Clinic located at Mulago National Referral Hospital is used as an instance of a real-life EA for a DH solution anchored on DHEAF.

IDI-Clinic, Mulago offers treatment to over 7,000 HIV patients and specialised clinics for special populations such as TB patients, pregnant women, adolescents, young adults, and discordant couples. Services offered by the clinic include; General clinic for HIV patients, Integrated TB-HIV clinic, Sexual and reproductive health services, Adolescents' Clinic, Discordant couples' clinic, Senior citizens clinic, Mental health clinic, non-communicable diseases clinic, Kaposi's sarcoma clinic, and Co-Pay clinic services.

To provide high-quality HIV services, the clinic implemented an electronic patient management system (ICEA) that records individual patient data, including all visits information. ICEA is linked to DHIS2, Uganda's National Health Information System, for collecting aggregated data on HIV and Navision Accountancy software to support in determining actual costs of patient care. The Clinic also uses RX solution to support pharmaceutical inventory management, including; drug ordering, stock taking, patient registration, prescription, dispensing of drugs, and audit. These solutions were, however, implemented without any kind of plan and coordination, which, resulted into several challenges including; (i) inaccurate and fragmented data; (ii) HIV/TB client management solution (ICEA) that is not fully aligned to all the client management processes at the clinic; (iii) increased workload for healthcare workers; (iv) duplication of services; and (v) inability to exchange data due to lack of standardisation.

IDI CMS Architecture Vision – to create a sustainable and interoperable digital health solution that supports the delivery of quality HIV/TB healthcare in a secure and cost-effective manner while meeting national and international healthcare standards.

The EA effort is limited to HIV/TB client management capability focusing on the following processes; Pre-test counseling, Client registration, Laboratory requisition, post-testing counseling, Baseline visits, visits, Follow-up clinical evaluation, Client referral, and Pharmacy management as seen in **Figure 16**.

EA REQUIREMENTS, OUTCOMES, AND GOALS

Table 22 summarises the enterprise architecture goals, requirements and outcomes for IDI clinic.

Table 22. IDI EA Requirements, Outcomes and Goals

Architecture Goals
• To make HIV/TB client care safer and more effective by making available the correct information in the right place at the right time.
• To ensure equitable access to quality healthcare services by all HIV/TB clients.
• To safeguard the confidentiality, privacy, and integrity of HIV/TB client health information.
• To ensure the seamless sharing of information to support health care delivery to HIV/TB clients.

Architecture Requirements
• Reduce redundancy, complexity, and duplication by optimising HIV/TB healthcare processes.
• Ensure interoperability of digital solutions that support HIV/TB client management
• Eliminate information silos
• Improve security and privacy of HIV/TB clients' data
Expected Outcomes
• *Improved client experience or satisfaction* - The HIV/TB CM) is implemented not as a tool for data collection but for delivering high-quality HIV/TB healthcare services to clients
• *Optimised HIV/TB client management processes* - Optimised HIV/TB healthcare processes will reduce complexity, redundancy, and duplication, making it easy to add new functions to support new requirements
• *Reduced cost*- With standards in place and improved integration and interoperability, it will be possible to re-use or integrate existing solutions rather than developing new ones, thereby reducing the cost of developing and maintaining new systems.
• Improved Security and Privacy of health data- By storing all HIV/TB clients' information in one system, it will be easy to manage access to the information

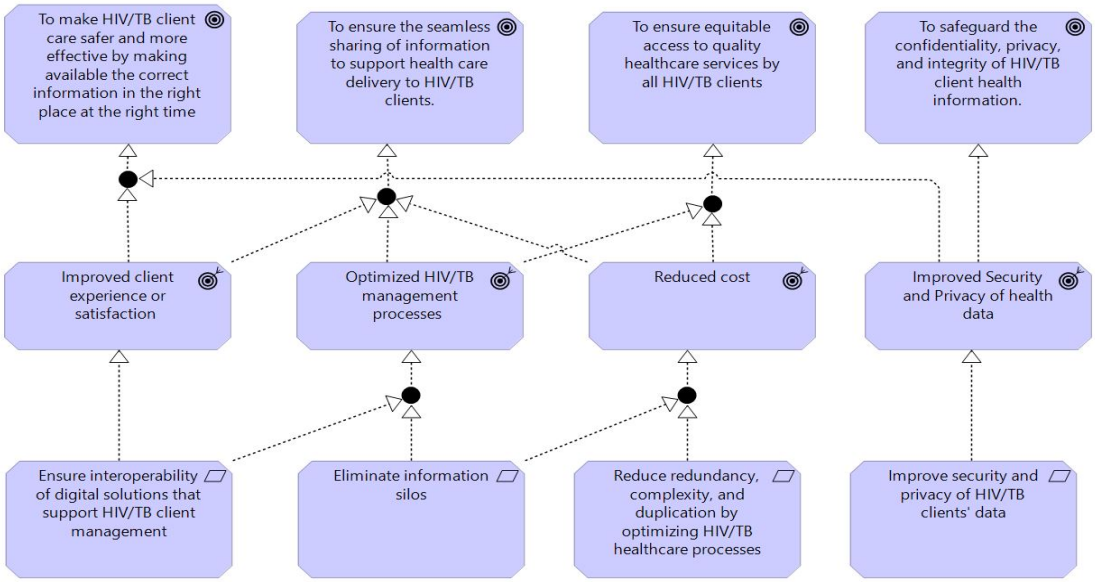


Figure 16: Goals, objectives, and requirements relationship diagram

ASSUMPTIONS, POTENTIAL RISKS, AND DEPENDENCES

Implementation of the target architecture for HIV/TB CMS will require the commitment and support of the leadership of the IDI clinic, Mulago, and all stakeholders. The benefits of the target architecture will only be realised once the architecture has been fully implemented. It is, therefore, critical to identify assumptions, anticipated risks, and dependencies to achieve this. **Table 23** summarises the assumptions, potential risks and mitigation measures to implement the architecture.

Table 23. Assumptions, Potential Risks and Mitigation Measures

Assumptions

Resources Availability	Leadership at the Clinic, shall ensure that the required financial and human resources are in place to support the implementation of the target HIV/TB client management architecture
Stakeholder Involvement	Implementers of the target architecture shall ensure that key stakeholders are involved in all the stages of the implementation process.
Leadership involvement and support	Leadership at the Clinic, shall drive the implementation of the target architecture, and will ensure that all employees comply with the new approach to service delivery.
Supportive technology infrastructure	Leadership at the Clinic, shall ensure the availability of the required technology infrastructure.

Potential Risks and Mitigation Measures

Code	**IDI_MR01**
Risk	***Change in leadership at IDI Clinic, Mulago.*** The current leadership at IDI-Clinic, believes that EA can be used as a general-purpose vehicle to transform HIV/TB client management. However, given the time it may take to have the target architecture implemented, changes in leadership may occur, and this may negatively affect the implementation of the target architecture
Probability	Medium
Impact	High
Mitigation approach	Implementers of the target architecture for HIV/TB client management should ensure that all top management members at IDI-Clinic, are involved in planning and directing the implementation of the target architecture such that if any one of them leaves, the other members can continue to support the implementation
Code	IDI_MR02
Risk	***Insufficient expertise in Enterprise Architecture*** EA is relatively new in Uganda, as such, the IDI-Clinic, may not have adequate staff trained in EA; which may affect implementation of the target architecture for HIV/TB Client Management
Probability	High
Impact	High
Mitigation approach	Management should organise in-house training in Enterprise Architecture for all the critical staff to be involved in the implementation of the target HIV/TB client management architecture
Code	IDI_MR03
Risk	***Resistance to new HIV/TB CMS.*** IDI-Clinic staff members who have been used to ICEA may not want to change to the new HIV/TB CMS.
Probability	Medium
Impact	High
Mitigation approach	Involve current users of ICEA in the development processes for the HIV/TB CMS.

DEPENDENCIES

ICT Governance – ICT Governance at the IDI-Clinic, should be strengthened to support the EA approach to digital transformation. New roles, including; Enterprise Architect, Data Standards Specialist, and Data Steward, should be added to the governance structure of the IDI-Clinic.

Knowledge about EA and Data Standards - Staff involved in the implementation of the target HIV/TB Client Management architecture should make efforts to upgrade their skills in EA, Interoperability, and data standards.

Resource mobilisation - Leadership at the IDI-Clinic, should work together to mobilise financial and human resources to support the implementation of the target HIV/TB client management architecture.

Information Management Principles – These include both the Enterprise principles (general rules intended to support decision-making at IDI-Clinic and shall dictate how the clinic plans to fulfill its mission) and Architecture principles *(business, data, application, technology, security and interoperability) that can be customised based on the generic DHEAF to suit IDI-Clinic CMS Architecture.*

Coding Standards

Table 24. Provides the recommended coding standards that should be followed in the implementation of HIV/TB CMS.

Table 25. Recommended Semantic Standards to Support HIV/TB CMS

Standard	Description	Recommendations
International Classification of Diseases (ICD)	A standard vocabulary for diseases, health status, types of patient visits to doctors and other health providers, and external causes of injuries.	HIV/TB CMS should use ICD 10 or 11 coding for disease specification.
Logical Observation Identification Names and Codes (LOINC)	A common terminology standard for Laboratory and clinical observations	HIV/TB CMS should use LOINC to define laboratory measurements and clinical observations.
Systematized Nomenclature of Medicine-Clinical Terms (SNOMED CT)	A standardised, multilingual vocabulary of clinical terminology used by physicians and other health care providers for the electronic exchange of clinical health information.	HIV/TB CMS should use SNOMED CT for clinical information.

INFORMATION SECURITY GUIDELINES

Table 26. Presents the guidelines for protecting and managing HIV/TB data.

Guideline	Description
Authentication	Use a password or combination of tokens, biometrics, or multiple authentications to control access to HIV/TB CMS.
Authorisation	Use of role-based access controls.
Encryption	Ensure that shared HIV/TB data is unreadable until an authorized user decrypts them.
Integrity	Ensure that HIV/TB data are protected from unauthorized alteration and destruction, whether accidentally or deliberately, and that data and programs are changed only in a specified and authorized manner.
Accountability	Track and monitor activities associated with the access and use of the HIV/TB CMS
Assurance and awareness	• Ensure that existing HIV/TB data is of high quality. • Monitoring and evaluation tools and procedures should be put in place to identify data quality issues that need to be addressed. • Ensure that user education is continuous for crucial staff interacting with HIV/TB CMS.
Auditing	Track all changes in access to HIV/TB data and all changes to the data.

HIV/TB CLIENT MANAGEMENT SYSTEM ARCHITECTURE INTEGRATED MODEL

ArchiMate modelling language is used to model the HIV/TB CMS Architecture as seen in **Figure 17**. *Archi*Mate offers an integrated architectural approach that describes, analyses, and visualises the different architectural domains and their underlying relations and dependencies (Josey, 2016). It is also fully aligned with TOGAF, the foundation standard for the development of the DHEAF.

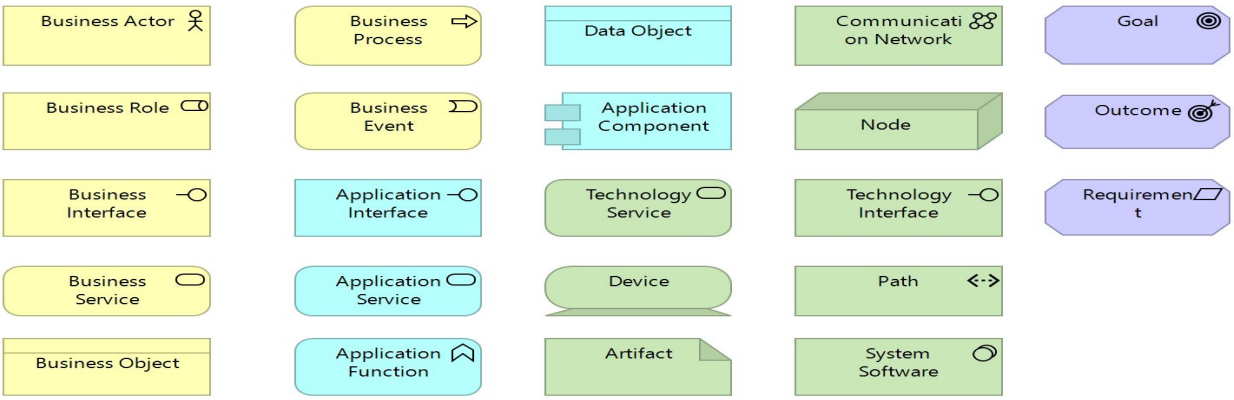


Figure 17. Modelling Language for HIV/TB Client Management System Architecture

Figure 18 below describes the key symbols used to document the HIV/TB CMS Architecture.

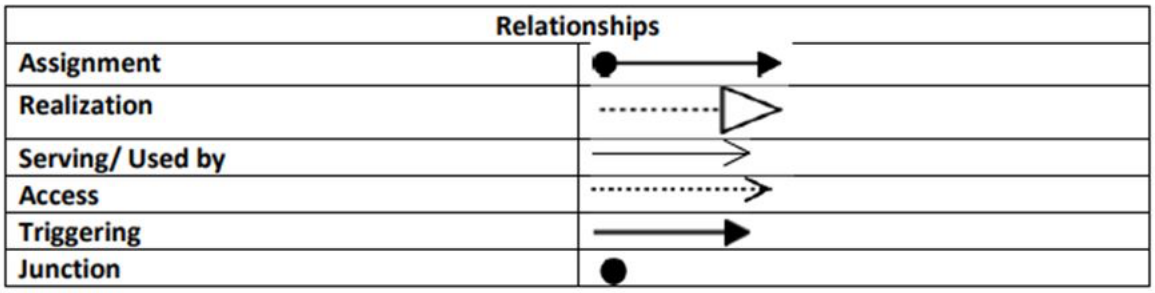


Figure 18. Symbols used in the CMS Architecture

Finally, the high-level HIV/TB Client Management System Architecture is presented in **Figure 19**.

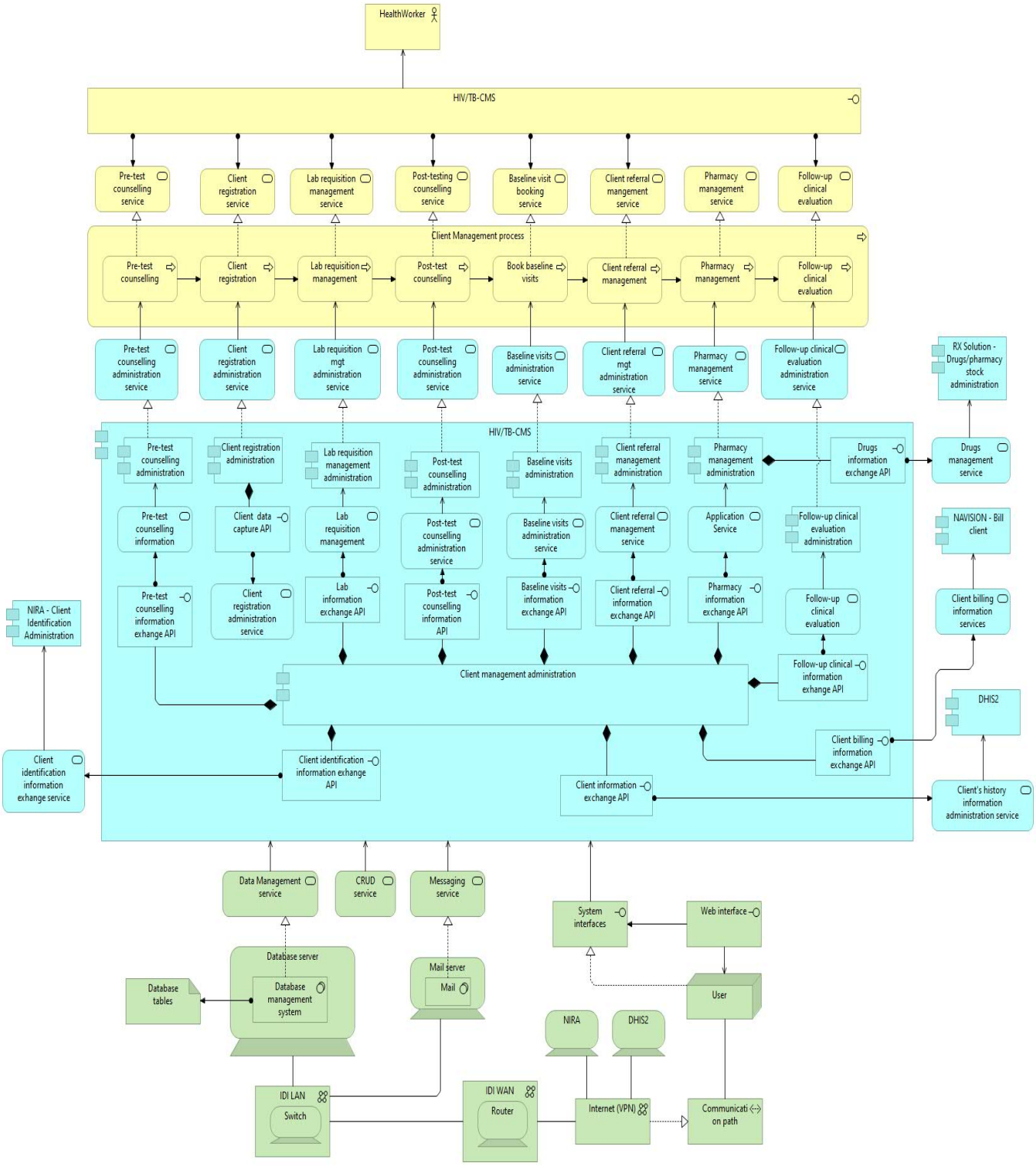


Figure 19. Integrated HIV/TB Client Management System Model (Initial version)

APPENDIX B.2: USE CASE – CONTEXTUALISING TERMINOLOGY CODES FOR HIV DISEASE MANAGEMENT SERVICES

Contextualisation of terminologies and medical codes follows a process as outlined in **Figure 20**. There has to be a need for a terminology to kick start the terminology contextualisation process. The need drives stakeholders to study the national and international health system contexts to understand the opportunities and complexities of the specific terminology. Understanding the national context will drive extraction of data sets and indicators from the national Health Information Systems. Mapping will consider the exact matches in terms of code descriptions and then unmatched codes will be contextualised using UG as a prefix to a code that is most similar in description in any of the international terminologies. Then a prefix that is serially labeled will follow as exemplified using HIV services in **Table 27**. The main terminologies that majorly suit our digital health ecosystem are Systematised Nomenclature of Medicine -- Clinical Terms (SNOMED-CT), International Classification of Diseases (ICD) and Logical Observation Identifiers Names and Codes (LOINC). SNOMED CT which is a structured clinical vocabulary for use in an electronic health record is the most comprehensive and precise clinical health terminology product in the world. ICD is designed to promote international comparability in the collection, processing, classification, and presentation of morbidity and mortality statistics. LOINC is a database and universal standard for identifying medical laboratory observations. The compiled terminologies will be validated with stakeholders and any revisions made if needed. The final set of terminologies will then be housed in an online terminology server housed at the Ministry of Health headquarters and managed by a standards manager.

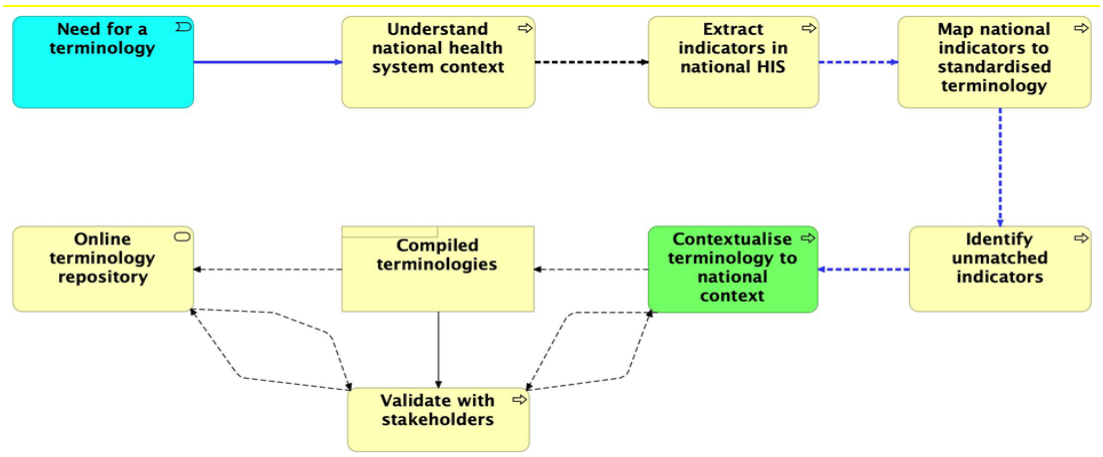


Figure 20. Process of Contextualising Health Terminologies

Terminology Codes for HIV Disease Management Services

Table 27. Use Case - Terminology Codes for HIV Disease Management Services

Terminology Code	Terminology Name	Terminology Description
Registry Codes		
Health Facility Registry	Name of Health Facility	Name of the health facility
Health Facility Registry	Code	Code of the health facility
Health Facility Registry	Level	Health system level of the health facility
Health Facility Registry	Sub-county / Division	Sub-county or division in which the health facility is located
Health Facility Registry	HSD	Health sub-district in which the health facility is located
Health Facility Registry	District	District in which the health facility is located
Health Facility Registry	Name of Health Facility	Name of the health facility
Health Facility Registry	District	District in which the health facility is located
Health Facility Registry	Hub	Hub for viral load testing
Health Worker Registry	Requesting Clinician	Clinician requesting for viral load analysis and HIV drug resistance testing
Health Worker Registry	Phone number	Phone number of the clinician requesting for viral load analysis and HIV drug resistance testing
Client Registry	NIN	National identification number of client
Client Registry	Patient's surname	Surname of the client
Client Registry	Patient's first name	First name of the client
Client Registry	Patient's contact	Telephone number of the client
Client Registry	Date of birth	Date of birth of the client
Client Registry	Sex	Sex of the client
Client Registry	Date of Birth	Date of birth of the client
Client Registry	Patient Clinic ID/ART #:	Unique identifier of client at the health facility
Client Registry	If DOB Unknown Age in Years	Age in years
Client Registry	If < 2 years, Age in Months	If the age is less than 2 years, indicate age in months
Client Registry	Sex	Sex of the client
Client Registry	NIN	National identification number of client
Client Registry	Other ID	Number of other identifications
Client Registry	Phone number	Telephone number of the client
Client Registry	If Pregnant, enter the ANC #	Antenatal care number of client
Client Registry	PNC #	Postnatal care number of client

Client Registry	Name of Exposed Person	Name of exposed person
Client Registry	Age	Age of exposed person
Client Registry	Sex	Sex of exposed person
Client Registry	Village	Village of exposed person
Client Registry	Parish	Parish of exposed person
Client Registry	Sub-county	Sub-county of exposed person
Health Worker Registry	Name of Lab Person	Name of laboratory personnel taking sample
Health Worker Registry	Phone number	Telephone number of laboratory personnel taking sample
Viral Load Codes		
76423-3	Date of Registration	Date of the first visit is considered the start date for a specific episode of care.
21866-9	Patient Clinic ID	Provides a unique identifier for the patient consisting of the year in which the patient was first seen at the reporting facility and the consecutive order in which the patient was abstracted. The first four numbers specify the year and the last five numbers are the numeric order in which the patient was entered into the registry database.
133932002	Supporter's name	Person in the healthcare environment to support the client
UGHIV.1137457010.0001	eMTCT	For female clients on eMTCT, write yes (Y) and then specify as "P" if Pregnant or "BF" if Breastfeeding
UGHIV.82772-6.0002	Date VL results received at facility	Date when viral load results were received at the facility as written on the result form
UGHIV.51953-9.0003	Date CD4 Sample Collected	Date CD4 collected from patient
8128-1	CD result / 100 cells	CD3+CD4+ (T4 helper) cells/100 cells in Blood
24467-3	CD4 result / volume in blood	CD3+CD4+ (T4 helper) cells [#/volume] in Blood
UGHIV.59419-3.0004	VL results at initiation of IAC (copies/ml)	HIV 1 RNA [#/volume] (viral load) in Plasma by Probe with signal amplification
UGHIV.20447-10.0005	VL results at initiation of IAC (copies/ml)	HIV 1 RNA [#/volume] (viral load) in Serum or Plasma by NAA with probe detection
UGHIV.21008-9.0006	VL results at initiation of IAC (copies/ml)	HIV 1 RNA [#/volume] (viral load) in Serum or Plasma by Probe
UGHIV.86548-6.0007	VL results at initiation of IAC (copies/ml)	HIV 2 RNA [#/volume] (viral load) in Plasma by NAA with probe detection
399445004	Date of sample collection	Date of sample collection
33882-2	Date of sample collection	Date of sample collection
UGHIV.133877005.0008	Regimen at VL test	Code of the ART regimen the patient is currently on
UGHIV.63936-10.0009	Start date of ARV Regimen	Date the client was initiated on the current regimen
UGHIV.413946010.0010	Start date of ARV Regimen	Date the client was initiated on the current regimen
104298002	Serum Crag Screening	Measurement of Cryptococcus species antibody (procedure)

31791-7	Crag Results	Cryptococcus sp Ag [Units/volume] in Serum
UGHIV.387174007.0011	Treated with Fluconazole	A client treated with fluconazole
UGHIV.95127-7.0012	TB LAM Test	TB LAM test done
UGHIV.95127-8.0013	TB LAM Results	TB LAM test result
UGHIV.45241-8.0014	TB Treatment	Is the client on TB treatment
UGHIV.409063006.0015	Restart Intensive Adherence Counselling (IAC)	"Yes" for a client who has completed 6 Intensive Adherence Counselling sessions but is not yet eligible for a Viral load re- test, and "No" for a client who is just starting Intensive Adherence Counselling.
UGHIV.409063006.0016	IAC session number	Indicate the Intensive Adherence Counselling session number
UGHIV.409063006.0017	Session date	The date the Intensive Adherence Counselling session was conducted
UGHIV.409063006.0018	Adherence assessment score (%)	The adherence assessment score in percentage
UGHIV.409063006.0019	Adherence code	The adherence assessment score (G for Good, F for Fair and P for Poor)
UGHIV.119297001.0020	VL sample collected	Sample collection for VL for clients on second line regimen
UGHIV.119297001.0021	HIVDR sample collected	Sample collection fo HIVDR
UGHIV.399445005.0022	Date of repeat VL / HIVDR sample collection	Date the repeat VL and HIVDR samples have been collected
UGHIV.59419-3.0023	Repeat VL results after IAC (Copies/ ml)	Repeat HIV-1 VL results after Intensive Adherence Counseling in copies per ml
UGHIV.56155-5.0024	Date VL Results Received at facility	Date VL results received at facility from referral lab
UGHIV.425581000.0025	HIVDR results	Results of HIVDR
UGHIV.56155-5.0026	Date HIVDR Results Received at facility	Date HIVDR results received at facility from referral lab
UGHIV.91541-3.0027	Clinical decision	Clinical decision after receiving VL and HIVDR results
UGHIV.133877005.0028	New Regimen	New treatment regimen using national codes
UGHIV.413946010.0029	Date of decision	Date clinical decision has been taken
86467-8	Comments	Narrative comments after the client's visit
406543005	Date	Date of visit
45235-9	Date of Treatment Initiation:	Date of starting HIV treatment
1C62.0	Current WHO Stage	HIV disease clinical stage 1
1C62.1	Current WHO Stage	HIV disease clinical stage 2
1C62.2	Current WHO Stage	HIV disease clinical stage 3
1C62.3	Current WHO Stage	HIV disease clinical stage 4

UGHIV.261773007.0030	How long has this patient been on the current regimen?	Duration the patient has been on current regimen
UGHIV.133877005.0031	Which treatment line is patient on?	Treatment line the client has been on
UGHIV.133877005.0032	Current Regimen	Current regimen the client is taking
77386006	Is mother pregnant?	Mother is pregnant
60001007	Is mother pregnant?	Mother is not pregnant
866041003	Is mother breastfeeding?	Mother currently breastfeeding
427099000	Patient has active TB?	Patient has active TB
UGHIV.45241-8.0033	If Yes, which phase are they on?	TB phase that the client is in
182884001	ARV Adherence	ARV adherence
UGHIV.182991003.0034	Treatment care approach	Treatment care approach as per the Differentiated Service Delivery Model
315124004	Indication for viral load testing	Indication for viral load testing
UGHIV.133877005.0035	Past Regimens	Past regimens that the client has taken as per the national guidelines
413946009	Start Date	Start date for the past regimens
413947000	Stop Date	Stop date for the past regimens
29463-7	Body weight (Kg)	Bodyweight of the client
UGHIV.387159010.0036	Patient on Rifampicin?	Patient taking rifampicin
68963-8	Date and Time of sample collection	Date of sample collection
118575009	Date and Time of Sample centrifugation	Date and Time of Sample centrifugation
20395-0	Sample type	Plasma sample type
57718-9	Sample type	DBS sample type
CRAG Register Codes		
406543005	Date	Date patient has come to health facility
76427-4	Date	Date patient has come to health facility
UG.64601-8.0037	Date of return after 1 week	Date of return for review after 1 week of Cryptococcal Antigen testing
UG.64601-8.0038	Date of return at 4 weeks	Date of return for review after 4 weeks of Cryptococcal Antigen testing
UG.64601-8.0039	Date of return at 3 months	Date of return for review after 3 months of Cryptococcal Antigen testing
UG.64601-8.0040	Date of return at 6 months	Date of return for review after 6 months of Cryptococcal Antigen testing

APPENDIX C.1: DH MONITORING & EVALUATION INDICATORS AND OPERATIONALISATION TOOLS

Indicator Domain	Measurement Means (Example Indicators)	Operationalisation Tools
Monitoring Programme / Digital Health Inputs and Activities (Does the Digital Health technology work?)		
Needs assessment	Availability of documentation of needs assessment results indicating public health needs to be addressed by the Digital Health and its alignment to strategic health objectives	Needs assessment reports
Functionality	The extent to which specified functionalities and requirements are met by the Digital Health technology Proportion of data fields from the original paper-based system that are captured by the Digital Health technology Proportion of the target population who report successful use of the Digital Health technology capabilities	Software testing outcomes System generated data User surveys
Software/ Application Standards requirements	Proportion of software standards requirements met by the Digital Health technology	Design specifications Software audit reports
Infrastructure requirements	Proportion of target population who are able to connect and use the Digital Health technology Proportion of target population with access to a power/electricity source for powering/recharging Digital Health related devices The extent to which required hardware technologies are met/provided by the Digital Health intervention	User surveys Infrastructure audit reports
Connectivity	Proportion of target population which can connect to the Digital Health technology signals	System generated data User surveys
User and technical support	Proportion of Digital Health intervention sites or users with access to local technical support for troubleshooting	User surveys
Human Resources	Proportion of target users that have been trained on the use of the Digital Health technology	Training reports
Financial Resources	Proportion of Digital Health budget that has been funded Proportion of Digital Health budget that has been timely funded	Budget Analysis reports
Management and political support	Proportion of Digital Health management stakeholders that commit their time or other resources in support of Digital Health implementation	Administrative data Surveys
Leadership and governance	Availability of an institutionalized Digital Health governance structure Proportion of Digital Health leadership positions that are occupied and functional	Administrative data
Sustainability	Availability of a sustainability plan for the implemented Digital Health Proportion of sustainability related actions that are completed Proportion of Digital Health implementation budget that is facilitated by local funding	Administrative data User surveys
Intervention documentation	Availability of an established systematic process for storage and maintenance of the Digital Health intervention documentation Availability and accessibility of the Digital Health initiative project charter Availability and accessibility of documented key steps from the Digital Health intervention's launch to pilot to maintenance and availability of an established systematic process for housing and maintaining such records	Administrative data
Readiness and change management	Availability of a change management strategy Proportion of change management related actions that are completed	Document reviews User surveys

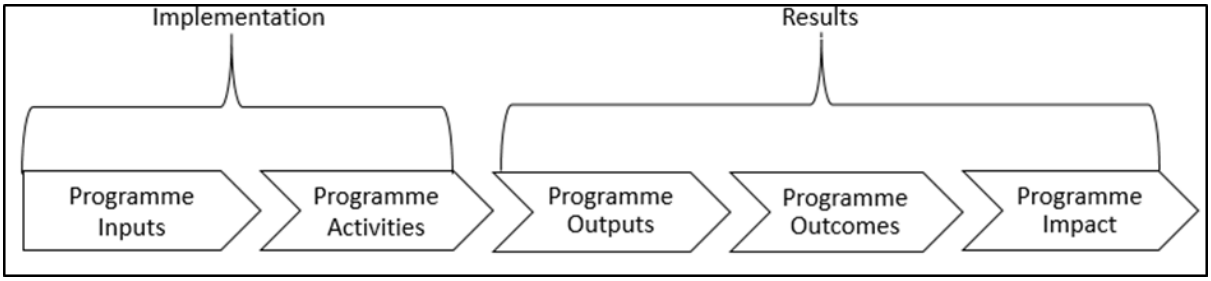
Legal and regulatory support	The extent to which available laws and regulations support and guide the implementation of Digital Health	Document reviews
Monitoring / Evaluating Digital Health Outputs (How do users interact with the Digital Health?)		
User Coverage	Proportion of users who demonstrate proficiency in use of Digital Health technology Proportion of target users observed using Digital Health system over a reference period	Observations System generated data User surveys
User representativeness	The proportionality of each target user category among users who demonstrate proficiency in use of Digital Health technology	User surveys
Transferability	Proportion of target population who report successful use of Digital Health technology capabilities The extent to which the Digital Health intervention has been adopted in different healthcare settings and usage scenarios	User surveys System generated data
User Response	Proportion of users who rate the Digital Health system as "easy to use" Proportion of users who rate the Digital Health system as 'works as intended' Proportion of users who report satisfaction with the content of health information received via the Digital Health system The extent to which users have a demand for the Digital Health	User surveys System generated data
User Adoption	Number of messages / reports / amount of data transmitted by end-users via the Digital Health technology within a reference period Proportion of messages / reports transmitted via the Digital Health system that are responded to appropriately by end-users over a reference period Proportion of data fields / forms / reports that are complete or left incomplete over a reference period	System generated data
Digital Health Outcomes (How does the Digital Health improve programme processes/service delivery? i.e. Evaluation)		
Patient Level		
Efficiency	Time between Digital Health system prompt received about a health intervention and seeking care from the provider Number of in-person consultations with qualified healthcare providers about a health intervention by target patients as a result of accessing required services using the Digital Health initiative over a reference period	Healthcare facility records, System generated data, Special surveys, Programme records
Quality	Time spent with a healthcare provider in relation to a health intervention at the last visit % of messages received through Digital Health intervention that patients are able to recall about a health intervention during patient exit interviews % of target patients who report correctly adhering to prescribed care protocol in relation to a health intervention % of target patients who report adverse effects from a health intervention % of target patients who report facing barriers to healthcare accessibility (health equity-related barriers)	Healthcare facility records, System generated data, Special surveys, Programme records
Utilization	% of emergency events where the Digital Health system was used by patients to expedite treatment over a reference period % of target patients who report receiving health information about a health intervention via the Digital Health system within a reference period % of target patients who report contact with a qualified healthcare provider using the Digital Health system in relation to a health intervention over a reference period % of target patients who report adequate knowledge about signs and symptoms for which they should seek care in relation to a health intervention % of target patients who report adequate knowledge about the health issue relevant to a health intervention	Healthcare facility records, System generated data, Special surveys, Programme records

Costs	% changes in reported patient out-of-pocket payments for illness management over a reference period	Healthcare facility records, System generated data, Special surveys, Programme records
Provider Level		
Efficiency	Time for last patient counselling about a health intervention using Digital Health system Time spent on health record-keeping about a health intervention over a reference period Time used per individual health worker over reference period to transmit data relating to a health intervention from community-based logs to health-care facility-based information systems Time taken per individual healthcare provider over a reference number of events between identification of an adverse event and provision of care (health intervention), across levels of a health system Time used per individual health worker to report important adverse events	Healthcare facility records, System generated data, Special surveys, Programme records
Quality	Proportion of health workers who report adequate knowledge of the health issue relevant to a health intervention Proportion of care standards relating to a health intervention observed to be met using the Digital Health initiative during a patient–provider consultation Proportion of providers observed to be using the Digital Health initiative during their patient consultations	Healthcare facility records, System generated data, Special surveys, Programme records
Utilization	Proportion of targeted health workers who use the Digital Health system in relation to a health intervention through the Digital Health system over a reference period Proportion of health workers observed to use the Digital Health system during their last client contact Proportion of health workers who use the Digital Health system to connect with medical staff to receive real-time clinical information and decision support Number of patients (average or total) attended by a health worker using the Digital Health system over a reference period	Healthcare facility records, System generated data, Special surveys, Programme records
Costs	Amount of estimated cost savings due to improvement in service delivery/efficiency/other factors related to using Digital Health	Healthcare facility records, System generated data, Special surveys, Programme records
Health System Level		
Efficiency	Cumulative time over a reference period for all health workers in a healthcare facility using the Digital Health system to enter data related to a health intervention Cumulative time over a reference period for all health workers to transmit data about a health intervention from community-based logs to healthcare facility information systems Cumulative time over a reference number of events between identification of an adverse event and provision of care (health intervention), across levels of a health system Number of days over a reference period for which a healthcare facility reports stock-out of a commodity essential for provision of a health intervention	Healthcare facility records, System generated data, Special surveys, Programme records
Quality	Number of health workers observed to be providing clinical services related to the Digital Health initiative % change in reported stock-out events of a commodity essential for provision of a health intervention over a reference period % change in data entry errors over a reference period	Healthcare facility records, System generated data, Special surveys, Programme records
Utilization	Number of patients seeking a health intervention over a reference period % of patients in a specified area who receive a health intervention through the Digital Health system over a reference period	Healthcare facility records, System generated data,

	% of target population who have access to a health intervention over a reference period % of health-care facilities in a target geographical area that use the Digital Health initiative Number of patients seeking a health intervention at a healthcare facility using the Digital Health system	Special surveys, Programme records
Costs	% change in costs of transporting paper forms and manual data entry over a reference period % change in costs of human resources for data entry % change in costs associated with timely and appropriate management of illness % change in reported patient out-of-pocket payments for management of illness Total population-level savings in out-of-pocket payments attributed to timely and appropriate care seeking	Healthcare facility records, System generated data, Special surveys, Programme records
Impact (How do improvements in service delivery impact health? i.e., Evaluation)		
Impact	Improvement in health outcomes attributed to the health intervention being supported by the Digital Health. Measures of health outcomes at this stage are defined basing on the expectations from a health intervention being supported by the Digital Health initiative. Examples of indicators include Mortality ratio, Mortality rate, Quality of life, Disease Incidence rate, Disease notification rate, Lifestyle	Population-based surveys, Coverage, Health status, Equity, Risk protection, Responsiveness

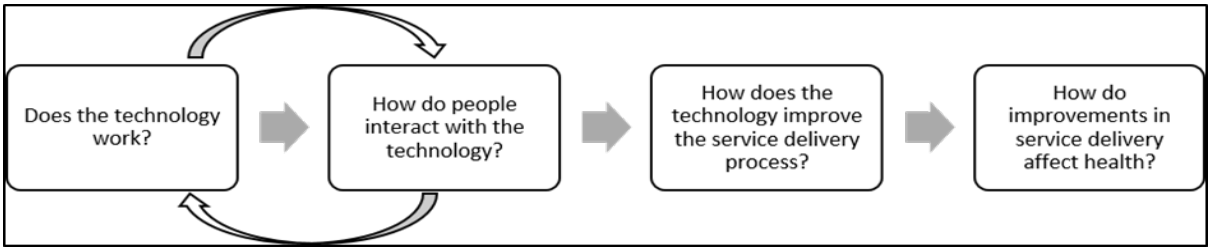
Source: Adopted from Ashaba & Nabukenya (2022)

APPENDIX C.2: RESULTS CHAIN BASED ON THE RESULTS-BASED MANAGEMENT STRATEGY



Source: UN Development Group (2011)

APPENDIX C.3: CATEGORISATION OF DH INDICATORS



Source: WHO (2016).