UNITED REPUBLIC OF TANZANIA

Ministry of Health, Community Development, Gender, Elderly and Children

Tanzania Health Enterprise Architecture

(TzHEA)

September 2020

Version 1

Contents

List of tables

List of figures

Abbreviations and acronyms

ADDO	accredited drug dispensing outlet
AIDS	acquired immunodeficiency syndrome
APHFTA	Association of Private Health Facilities in Tanzania
API	application programming interface
BAKWATA	Baraza Kuu la Waislamu Tanzania
BI	business intelligence
CBO	community-based organization
CHF	community health fund
CHMT	council health management team
CPD	continuing professional development
CRVS	civil registration and vital statistics
CSSC	Christian Social Services Council
DCS	Directorate of Curative Services
DNS	Domain Name System
DOS	desktop operating system
DPG	Development Partners' Group
DPS	Directorate of Preventive Services
EA	enterprise architecture
EHPRC	Environmental Health Practitioner Registration Council
ESB	enterprise service bus
e-GA	e-Government Authority
FBO	faith-based organization
GoT	Government of Tanzania
HCMIS	Human Capital Management Information System
HIS	health information system
HLPC	Health Laboratory Practitioners' Council
HMIS	health management information system

HIV	human immunodeficiency virus
HR	human resources
HRH	human resources for health
HSSP	Health Sector Strategic Plan
ICD-10	*International Classification of Diseases, Tenth Revision*
ICT	information and communication technology
IDSR	Integrated Disease Surveillance and Response
IEC	information education and communication
IEC	International Electrotechnical Commission
IP	Internet Protocol
IS	information system
ISO	International Organization for Standardization
IT	information technology
LGA	local government authority
M&E	monitoring and evaluation
MCT	Medical Council of Tanganyika
MIS	management information system
MoFP	Ministry of Finance and Planning
MoHCDGEC	Ministry of Health, Community Development, Gender, Elderly and Children
MoLCA	Ministry of Legal and Constitutional Affairs
MoWTC	Ministry of Works, Transport and Communications
MRIPC	Medical Radiology and Imaging Professional Council
MSD	Medical Stores Department
NACTE	National Council for Technical Education
NBS	National Bureau of Statistics
NBTS	National Blood Transfusion Service
NDHS	National Digital Health Secretariat
NDHSC	National Digital Health Steering Committee

NECTA	National Examinations Council of Tanzania
NGO	nongovernmental organization
NHIF	National Health Insurance Fund
NIDA	National Identification Authority
NIMR	National Institute of Medical Research
NOS	network operating system
ORM	object-relational mapping
OC	Optometry Council
OS	operating system
PC	Pharmacy Council
PHAB	Private Health Accreditation Board
PHLB	Private Health Laboratories Board
PMO	Prime Minister's Office
POPSM&GG	President's Office–Public Service Management and Good Governance
PORALG	President's Office–Regional Administration and Local Government
PPM	planned preventive maintenance
RHMT	regional health management team
RRHMT	regional referral hospital management team
RITA	Registration Insolvency and Trusteeship Agency
SDP	service delivery point
SWAp	sector-wide approach
TAMPC	Traditional and Alternative Medicine Practitioners' Council
TASAF	Tanzanian Social Action Fund
TBS	Tanzania Bureau of Standards
TCRA	Tanzania Communication Regulatory Authority
TC-SWAp	Technical Committee Sector-Wide Approach
TCU	Tanzania Commission for Universities
TFNC	Tanzania Food and Nutrition Council
TIRA	Tanzania Insurance Regulatory Authority

TMDA	Tanzania Medicines and Medical Devices Authority
TNMC	Tanzania Nurses and Midwives Council
TOGAF	The Open Group Architecture Framework
TWG	Technical Working Group
TZHEA	Tanzania Health Enterprise Architecture
VPN	virtual private network
W3C	World Wide Web Consortium
WCAG	Web Content Accessibility Guidelines
WHO	World Health Organization
XML	Extensible Markup Language

Definitions

The Tanzania Health Enterprise Architecture (TZHEA) uses the following definitions:

1. ***Confidentiality***
   The status accorded to data or information indicating that it is sensitive for some reason and therefore needs to be protected against theft, disclosure, and improper use and must be disseminated only to authorized individuals or organizations with a need to know.

2. ***Privacy***
   The right to maintain control over personal information.

3. ***Security***
   Processes and measures used to protect data from unauthorized access and data corruption throughout its life cycle. These include data encryption, tokenization, and key management practices that protect data.

4. ***System security***
   The totality of system safeguards, including hardware, software, personnel policies, information practice policies, disaster preparedness, and oversight of these components. Security protects both the system and the information contained within it from unauthorized access from without and from misuse from within.

5. ***Telemedicine***
   The provision of health care services and education over a distance using telecommunication technologies.

6. ***Digital health solutions***
   A digital product or service, or a combination of multiple products or services, created to serve a specific health system objective. It often encompasses a set of information and communications technology infrastructure and services required to improve the effectiveness and efficiency of the health system.

7. ***Health system***
   Consists of all organizations, people, and actions whose primary intent is to promote, restore, or maintain health. This also encompasses the people, institutions, resources, and policies that governments put in place to improve public health.

Foreword

A healthy population is necessary for the prosperity of the Tanzanian economy. In order to achieve universal health coverage and high-quality health care, the Government of Tanzania has been implementing the Health Sector Strategic Plans as well as a range of detailed supporting strategies. There has been remarkable progress in the health status of Tanzania. Despite the progress achieved, there are still challenges to be addressed in improving the health of the population, the quality of care, and the inequalities in access and service.

In recent years, digital health has gained a lot of traction as an engine for innovation to attain universal health coverage. Digital technologies have significant potential to transform health care services in ways that contribute to health-sector goals, including quality and continuity of health care services, efficient use of resources, supported availability, and use of high-quality health information. The Government recently launched, and has begun implementing the Digital Health Strategy 2019–2024.

In order for digital information systems to facilitate the achievement of health-sector goals and objectives, systems must be designed to support health-sector processes, to seamlessly work together, and to share information as appropriate, while ensuring client safety data security, confidentiality, and privacy.

The Tanzania Health Enterprise Architecture lays out how different digital systems will seamlessly work together to support health-sector processes across different health-sector institutions. It outlines standards to be adhered to so that digital systems can effectively work together to support health-sector objectives.

This document is part of the Government's ongoing efforts to ensure that digital health information systems are deployed and implemented in a well-coordinated and interoperable manner. It outlines how "shared digital services," such as registries and terminology services, will allow different systems to speak the same language and exchange information, as appropriate. The Government has already implemented a health facility registry to ensure all systems can reference and identify health facilities in a consistent way. It is currently developing other shared digital services to ensure that health clients (patients) and health workers can be tracked across systems, and that standard terminology is used to refer to health data.

Enterprise architecture shows how shared digital services and technology can support digital applications, how digital applications can support better information, and how better information can support and enable better achievement of health sector objectives.

I call upon all public and private health-sector stakeholders to ensure that their digital health initiatives and systems are aligned with the Digital Health Strategy 2019–2024, Digital Health Investment Roadmap 2019–2024, and the enterprise architecture and standards outlined in this document.

Prof. Mabula D. Mchembe
Permanent Secretary (Health)

Acknowledgements

The Tanzania Health Enterprise Architecture blueprint has been developed to provide standards for information exchange and to guide how different digital systems will work together to support health sector processes and institutions. It will help organizations align their information systems with the health sector's mission, goals, and objectives.

In developing this blueprint, an intensive and comprehensive consultative process has been employed with health sector stakeholders at different levels.

The Ministry of Health, Community Development, Gender, Elderly and Children extends its sincere gratitude to all the stakeholders involved for their valuable technical contributions during the development process for this blueprint.

I would like to recognize and appreciate the contributions of members of the task team who were engaged from the beginning of the development process. The task team represents different players from across the health sector. It includes representatives from the Ministries, Departments and Agencies; regional administrative secretaries; regional health management teams; council health management teams; district information communication technology officers; hospital management teams from both public and private hospitals; training institutions; professional councils; regulatory bodies; vertical programs; and development and implementing partners.

The Ministry of Health, Community Development, Gender, Elderly and Children expresses special appreciation to PATH for its technical support for development of the first Tanzania Health Enterprise Architecture blueprint. The ministry is grateful to government officials at the Ministry of Health, Community Development, Gender, Elderly and Children and the President's Office–Regional Administration and Local Government for their coordination, overall guidance, and tireless technical support throughout the development of this blueprint.

I wish to acknowledge the support of all individuals and institutions not explicitly mentioned here that have contributed to the accomplishment of this work. Your invaluable contributions and efforts are highly appreciated.

I would like to specifically acknowledge the contributions of the chief architect, Dr. Henry Mwanyika, together with the Department of Policy and Planning and the Information Communication Technology team of the Ministry of Health, Community Development, Gender, Elderly and Children, which worked tirelessly together to lead the task team during the development of the blueprint.

The ministry remains committed to the dissemination and implementation of the blueprint at all levels of the health sector.

Prof. Abel N. Makubi
Chief Medical Officer

1 Introduction

1.1 Background

Enterprise architecture (EA) is an approach that organizations can use to help align their information system (IS) with their mission, goals, and objectives and help them determine how to most effectively achieve their objectives by investing in information and communication technology (ICT). EA applies principles and practices to guide organizations through the business, IS, and technology changes necessary to execute their strategies. The EA approach can help the health sector simplify the complexity of its health information system (HIS) by identifying important relationships and aligning different components of the HIS to reduce the risks of fragmentation, duplication, and lack of interoperability.

The World Health Organization (WHO) recognizes EA as a method of assessing or describing technology adoption in the health sector. For member countries to achieve HIS improvement, WHO recommends the following development steps: architecture vision, business architecture, IS architecture, technology architecture, opportunities and solutions, migration planning, implementation governance, and architecture change management.[i]

In line with WHO and other global standards, Tanzania first articulated its intent to use EA to manage digital transformation in the health sector in its first national eHealth strategy (2013–2018). Through its Ministry of Health, Community Development, Gender, Elderly and Children (MoHCDGEC), the Government of Tanzania (GoT) aimed to use EA to guide the development of an integrated national HIS. The need for the health sector to apply the EA approach is also evident in Tanzania's draft National Health Policy (2020), which aims "to achieve improved efficiency of the Health Management Information Systems (HMIS) and its associated processes to meet health-sector monitoring and evaluation requirements." The need for the EA approach is further emphasized in the country's Digital Health Strategy 2019–2024.

The GoT is applying the EA approach to manage digital transformation in the health sector. EA is structured around four goals: efficiency, effectiveness, agility, and durability. These goals determine how the EA blueprint and concepts are developed, implemented, and governed. The EA provides an overview of how the health sector in Tanzania operates and determines how the sector can most effectively achieve its current and future objectives through digital health solutions.

1.2 Problem description

The health sector in Tanzania is among the sectors with the widest range of stakeholders and initiatives. As productive as it can be to have a wide range of stakeholders, this has led to duplicative efforts, inefficient use of resources (due to inappropriate collaboration), and implementation of pilot health initiatives with unsuccessful scale-up and sustainability plans. The GoT and other stakeholders are continuing to invest in various digital health solutions. However, without some form of national plan and coordination there is a risk of continued duplication of efforts, ineffective investments, creation of solutions that cannot be integrated or scaled across the continuum of care, and increased workload for health providers.

The Tanzanian health sector is characterized by a fragmented landscape of pilot projects and numerous siloed digital solutions, with significant barriers to the effective sharing of information among these solutions. As of 2019, more than 160 distinct health-related data systems were operating in Tanzania, according to the Tanzania Digital Health Strategy 2019–2024. These systems have contributed to several challenges in the health sector, including (i) inaccurate and fragmented data; (ii) lack of common, structured, and accessible standards for health terminology, such as diagnosis and drugs; (iii) inflexible systems and processes; (iv) duplication of effort; and (v) inability to exchange data due to lack of standardization.

Digital health solutions are meant to facilitate and enhance clients' experience at service delivery points (SDPs) by improving business processes and supporting data-driven decision-making. If not well-coordinated, integrated, documented, and backed by required infrastructure, digital health solutions may end up causing problems and may not align with the health sector's vision, mission, and objectives.

1.3 Document purpose

The purpose of this document is to guide the process of planning, designing, developing, rolling out, and supporting and maintaining digital health solutions in the Tanzanian health sector. It also provides a way to align digital health solutions with the sector's strategic priorities and its vision, mission, and objectives. In addition, it describes data flows and standards, including technology standards that should be followed when implementing digital health solutions.

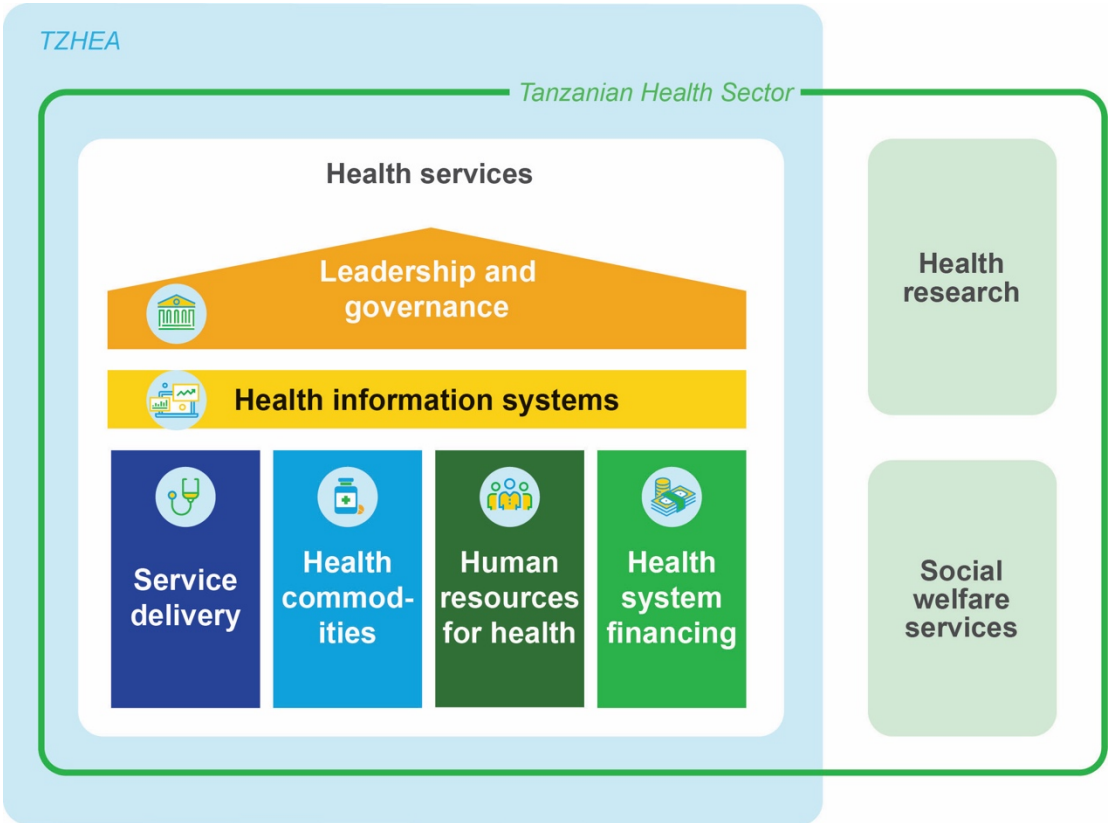
1.4 Tanzania Health Enterprise Architecture

The Tanzania Health Enterprise Architecture (TZHEA) is a blueprint for facilitating alignment of the health sector's strategies and operations with digital health solutions.

1.4.1 Scope

The TZHEA identifies three dimensions of Tanzania's health sector: health services, social welfare services, and health research. The TZHEA focuses on the health services dimension, which encompasses the six health system building blocks identified by WHO: service delivery, health commodities, health financing, human resources for health (HRH), leadership and governance, and HISs (Figure 1).

Figure 1. Scope of the Tanzania Health Enterprise Architecture.



1.4.2 TZHEA business drivers

The following key business drivers led to the development of the TZHEA:

1. ***Eliminate duplication of efforts***—by providing a unified framework for developing and documenting digital solutions that address mission-specific requirements and adhere to the GoT's standards and reporting needs.

2. ***Provide a common frame of reference***—by developing a frame of reference that the GoT can use to contract service providers or steer the development of digital health solutions in a cohesive manner.

3. ***Increase cost savings***—through targeted and informed allocation of resources to promote sustainability and the integration of digital health solutions.

4. ***Increase business and information technology (IT) alignment***—through IT investments that contribute to the health sector's vision, mission, and objectives.

5. ***Eliminate siloed systems***—by identifying and defining use cases for integration of systems and interoperability and creating a road map for TZHEA implementation, governance, and standards.

1.4.3 Vision

The vision of the TZHEA is "to simplify the complexity of Tanzania's health information systems and accelerate the application of innovative interoperable technologies to improve the efficiency, agility, durability, and effectiveness of the health system by ensuring the right data are available at the right time to the right people for evidence-based actions."

1.4.4 Expected outcomes

The following are the expected outcomes of successful implementation of the TZHEA:

1. ***Improved client experience or satisfaction***
   Digital health solutions will be designed and developed not as tools for data collection but as tools to facilitate delivery of high-quality health services.

2. ***Efficient processes***
   Improved business processes and their application will result in better alignment with priorities outlined in the health sector's strategic plans.

3. ***Reduced cost***
   With standards in place and improved integration and interoperability, the health sector will be in a position to reuse or integrate existing solutions rather than developing new ones, thereby reducing the cost of developing and maintaining new systems.

4. ***Achievement of strategic goals***
   Better alignment of digital health investments with the health sector's strategic plans will ensure that investments support the health sector in meeting its objectives.

2 Methodology

The GoT, through the MoHCDGEC and the President's Office–Regional Administration and Local Government (PORALG), developed the TZHEA blueprint in close collaboration with stakeholders at all levels. Stakeholder involvement, facilitated by the TZHEA development team, known as the "task team," helped ensure that the blueprint would take into consideration stakeholders' concerns and incorporate their input on the desired target architecture.

Stakeholders reviewed existing processes (including by walking through the flow of existing processes) and challenges and recommended improvements after consulting with subject matter experts (SMEs). They also reviewed guidelines and regulations to determine their effectiveness in supporting existing processes, tools, and systems. In addition, they reviewed tools and systems to determine how standards and existing features supported health-sector operations and management.

2.1 Reference models and framework

The development of the TZHEA was guided by standards and technical guidelines developed by Tanzania's e-Government Authority (e-GA) and The Open Group Architecture Framework (TOGAF®) Standard (TOGAF is a registered trademark of The Open Group).[ii] The TZHEA was also developed in compliance with other GoT guidelines, including *Guidelines for Appropriate and Secure Use of ICT in the Government*, which was issued by the President's Office–Public Service Management and Good Governance (POPSM&GG).

2.1.1 e-GA standards

The e-GA standards and guidelines referenced during the development of the TZHEA include:

1. ***e-Government Business Architecture – Standards and Technical Guidelines***[iii]—referenced for guidance on documentation and assessment of current and target business processes. Guidelines focus on the delivery of services by government entities that are critical, flexible, and sensitive to citizen needs.

2. ***e-Government Information Architecture – Standards and Technical Guidelines***[iv]—referenced for guidance on data creation, availability, ownership, security and confidentiality, archiving and retention, use of common data, and metadata definition and standards.

3. ***e-Government Infrastructure Architecture – Standards and Technical Guidelines***[v]—referenced for guidance on storage and network infrastructure, software licensing, ICT disaster recovery and business continuity, ICT vendor management, human resources, and service management.

4. ***e-Government Interoperability Framework – Standards and Technical Guidelines***[vi]—referenced for guidance on information sharing, collaboration, integration of systems, and the use of common open standards.

5. ***e-Government Security Architecture – Standards and Technical Guidelines***[vii]—referenced for guidance on how to securely and economically protect public institutions from security threats while maintaining compliance with the security and legal requirements for confidentiality, privacy, accessibility, availability, and integrity.

6. ***e-Government Integration Architecture – Standards and Technical Guidelines***[viii]—referenced for guidance on how applications are integrated to enable real-time, seamless information exchange.

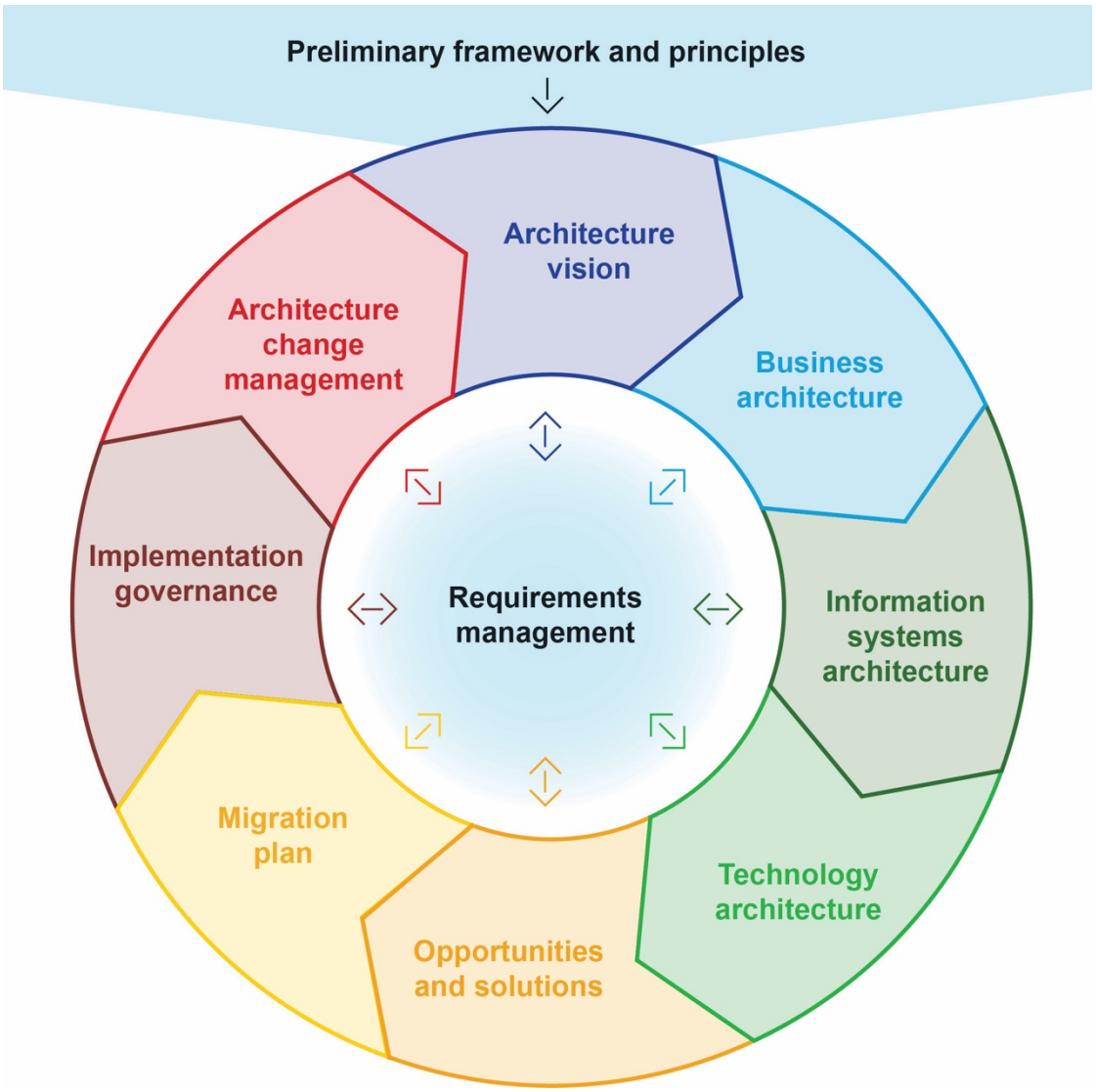
7. ***e-Government Process and Governance – Standards and Technical Guidelines***[ix]—referenced for its recommended governance mechanisms through which e-Government-related standards and guidelines can be initiated at the national level and adopted and implemented at the public institution level.

2.1.2 TOGAF Standard

The TOGAF Standard is a detailed method and set of supporting tools for developing an EA. TOGAF follows the Architecture Development Methodology, which is a step-by-step process for developing or modifying an EA.

Figure 2 shows the steps of the development process defined in the TOGAF framework, as adapted for the TZHEA development process.

Figure 2. Tanzania Health Enterprise Architecture Development Methodology (adapted from TOGAF).

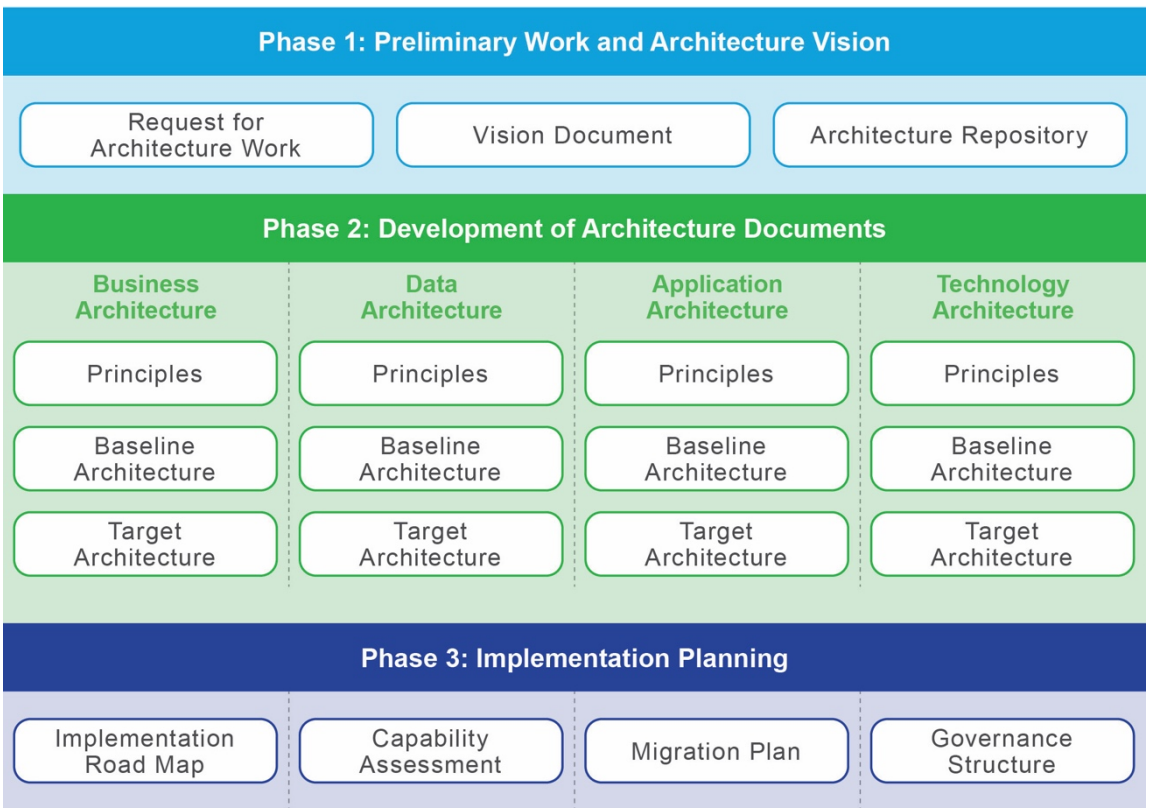


2.1.3 Deliverable framework

The deliverable framework describes the main deliverable phases of developing the TZHEA. The first phase was preliminary work, including developing a request for architecture work (establishing the need for the TZHEA) and a vision document (establishing a common understanding among stakeholders and outlining TZHEA objectives and outcomes). The second phase involved developing more detailed documents, or "architecture artifacts," for business, data, application, and technology domains. The third phase focused on what needed to be done for TZHEA implementation to be successful, including creating an implementation road map, capability assessment, migration plan, and governance structure.

Figure 3 depicts the deliverable framework for developing the TZHEA.

Figure 3. The Tanzania Health Enterprise Architecture deliverable framework.



2.2 Stakeholder engagement

The GoT, through the MoHCDGEC and in collaboration with PORALG, led the TZHEA task team, which engaged stakeholders from all levels of the health system to ensure that the TZHEA would respond to the real needs of the users and also build a broad sense of ownership and acceptance. Representatives from council health management teams (CHMTs) and regional health management teams (RHMTs) represented clients (patients) during the TZHEA development process. This approach was crucial to ensuring that the architecture would focus on improving the client experience and on how the health system would address their needs.

To ensure that the TZHEA development process would be informed by input from health-sector stakeholders, the task team was divided into six subcommittees mirroring WHO's six building blocks: service delivery, health commodities, human resources for health, health system financing, leadership and governance, and health information systems. Members of these subcommittees were selected from within the MoHCDGEC, PORALG, the Ministry of Finance and Planning, the Prime Minister's Office (PMO), and the POPSM&GG. Subcommittee members also included stakeholders from other public and private institutions, including the Medical Stores Department (MSD), research institutions, and academic institutions. Subcommittee members and other stakeholders engaged in a number of workshops to review the health sector's functions, services, processes, and key challenges. Appendix B lists the organizations that participated in the development of the TZHEA.

2.3 Use of local subject matter experts

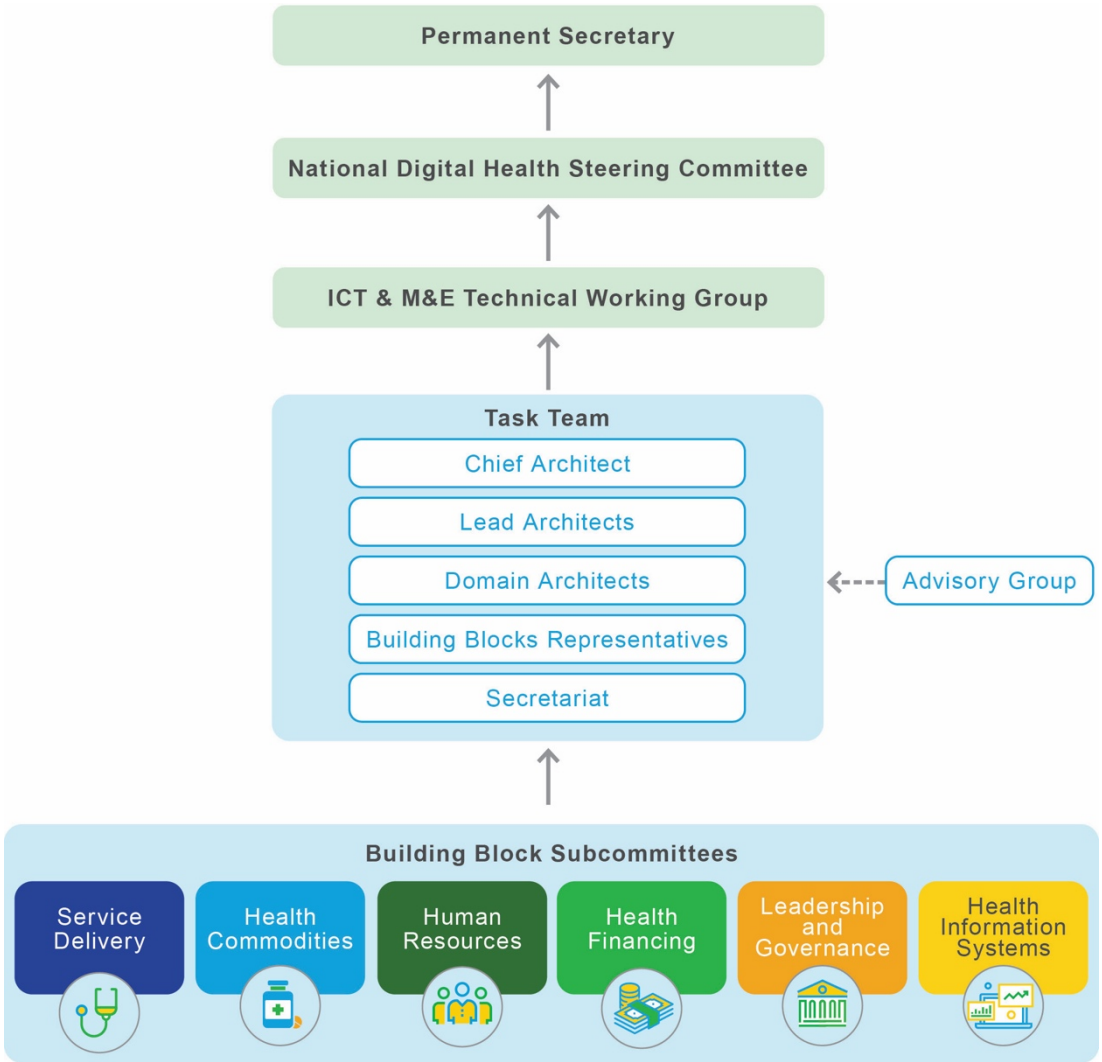
The GoT invested in training and certifying selected officials from the MoHCDGEC and PORALG on TOGAF and other EA-related frameworks. These officials guided the task team during the development process.

2.4 Governance structure

The task team comprised a chief architect, lead architects, domain architects (for the business, data, application, and technology domains), and two subject matter expert representatives from each building block subcommittee. (These subcommittees, which included subject matter experts and government leaders with expertise in each building block area, advised the task team.)

The task team reported to the Advisory Group, which comprised heads of departments and units from the MoHCDGEC, PORALG, and e-GA. All deliverables from the TZHEA task team were shared with members of the ICT and Monitoring and Evaluation (M&E) Technical Working Group (TWG) and the National Digital Health Steering Committee (NDHSC). The MoHCDGEC Permanent Secretary approved the final document. Figure 4 depicts the governance structure for the development of the TZHEA.

Figure 4. Governance structure for development of the Tanzania Health Enterprise Architecture.



Abbreviations: ICT = information and communication technology; M&E = monitoring and evaluation; TWG = Technical Working Group.

3 Assumptions, risks, and dependencies

Development and implementation of the TZHEA are continuous endeavors that require commitment from the GoT and its stakeholders. The benefits of the TZHEA will be realized once the architecture is successfully implemented. To achieve this, it is critical to identify assumptions, anticipated risks, and dependencies.

3.1 Assumptions

Successful implementation of the TZHEA is based on the following assumptions:

1. ***Resource availability***
   Financial and human resources will be adequate.

2. ***Stakeholder engagement***
   Stakeholders will be committed and supportive.

3. ***Endorsement from decision-makers***
   Decision-makers will provide continued interest, drive, and endorsement.

4. ***Continuous updates***
   The TZHEA is a living document that will be continually updated to reflect changes in health-sector priorities.

5. ***Understanding of the EA***
   The TZHEA task team will continuously build capacity for implementation.

6. ***Supportive infrastructure***
   Infrastructure will be in place to support implementation of digital health solutions.

7. ***Successful migration of legacy systems***
   Legacy systems will be smoothly migrated, with minimal interruption of business operations.

3.2 Risks

Table 1 shows the potential risks of implementing the TZHEA, along with strategies for mitigating them.

Table 1. Potential risks of the Tanzania Health Enterprise Architecture and mitigation strategies.

Risk	Probability	Impact	Mitigation strategy
Change in sector leadership priorities Given the time it may take for the impact of the TZHEA to be realized, changes in leadership may occur that negatively affect knowledge of and interest in the TZHEA.	Medium	High	+ From the preliminary stage to the implementation stage, the TZHEA development process has been led and fully owned by the government. + The TZHEA is included in the orientation of new leaders.
Inadequate expertise in enterprise architecture The concept of enterprise architecture is relatively new in Tanzania, so a lack of experts in EA at different levels of the government may affect implementation of the TZHEA.	High	Medium	+ MoHCDGEC and PORALG staff are trained as certified architects and TZHEA champions as well as national-level trainers of trainers. + Various agencies and stakeholders are encouraged to align their ICT policies and strategies with the TZHEA guidelines and standards and are supported in doing so.

Abbreviations: EA, enterprise architecture; ICT, information and communication technology; MoHCDGEC, Ministry of Health, Community Development, Gender, Elderly and Children; PORALG, President's Office–Regional Administration and Local Government; TZHEA, Tanzania Health Enterprise Architecture.

3.3 Dependencies

The dependencies for successful implementation of the TZHEA include:

1. ***Governance structure to support the TZHEA***
   This includes a well-functioning TZHEA Subcommittee linked to the ICT and M&E TWG with a mechanism for reporting to the NDHSC. The subcommittee should have the power to enforce TZHEA recommendations among stakeholders in the health sector.

2. ***Knowledge about digital solutions and ICT***
   Some of the recommended digital solutions will require staff with a certain level of understanding of digital solutions, ICT in general, and use of data and digital tools to optimize business processes and improve efficiency.

3. ***Resource mobilization***
   The GoT and stakeholders should work together to mobilize resources to support implementation of the TZHEA.

4 Business architecture

This chapter describes how the health sector in Tanzania is structured and works toward its goal of creating a healthier society. It describes the current state of the health sector; its vision, mission, and objectives; key stakeholders; and the governance structure. The baseline business architecture is the current setup of stakeholders, business processes, and key challenges facing the health sector. The target business architecture is the set of proposed business processes that may use digital health solutions to improve efficiency.

4.1 Health-sector vision, mission, and objective

Vision

"A healthy community that contributes effectively to the individual as well as to the nation's development towards becoming a middle-income country."[x]

Mission

"Facilitate the provision of basic health services that are of good quality, equitable, accessible, affordable, sustainable and gender-sensitive."[x]

Objective

"To reach all households with essential health and social welfare services, meeting, as much as possible, the expectations of the population, adhering to objective quality standards, and applying evidence-informed interventions through efficient channels of service delivery."[xi]

4.2 Architecture principles

Architecture principles are guiding rules for managing business processes and functions. Table 2 summarizes the TZHEA business architecture principles.

Table 2. Tanzania Health Enterprise Architecture business architecture principles.

Principle	Health-sector focus (primary principle)
Reference code	TZHEA-P01
Statement	Information technology decisions should be made based on the needs of, and benefits to, the health sector as a whole.
Rationale	To ensure adequate and consistent information for all stakeholders and decision-makers and the realization of their business goals and their purpose: the provision of high-quality health care services for sector-wide benefits.
Implications	+ All individuals and institutions within the health sector should work for the benefit of the health sector. If what appears to be best for the organization might not work well for the sector, priority should be given to what will work for the sector. + Digital health initiatives should not be embarked upon until they are examined for compliance with the principles outlined in the Tanzania Health Enterprise Architecture and other relevant policies, strategies, and guidelines. + Principles should be amended in accordance with the prevailing decision-making process.
Principle	**Alignment of digital health with the health sector**
Reference code	TZHEA-P02
Statement	Decisions regarding digital health should be made in alignment with business objectives in order to maximize benefits for the health sector and for clients as the primary beneficiaries.
Rationale	To ensure that decisions and plans about digital health initiatives are made with greater consideration for and alignment with the health sector's vision, mission, and objectives.

Implications	All digital health initiatives should add value to the health sector.
Principle	**Maximum benefits at the lowest cost and lowest risk**
Reference code	TZHEA-P03
Statement	Strategic decisions about digital solutions should aim to maximize benefits to clients while ensuring the lowest cost and minimal risk.
Rationale	To assess every strategic decision based on costs, risks, and benefits.
Implications	+ Digital health solutions should be based on a qualitative or quantitative assessment of costs, risks, and benefits. + Information technology infrastructure should be optimized based on business requirements, implementation costs, and risks.
Principle	**Business continuity**
Reference code	TZHEA-P04
Statement	Health service delivery should continue uninterrupted despite any information system issues.
Rationale	To continue health operations despite software and/or hardware failures that may occur as business processes and functions are digitized and dependencies on digital health solutions are created.
Implications	Information system failures should not affect provision of health services.

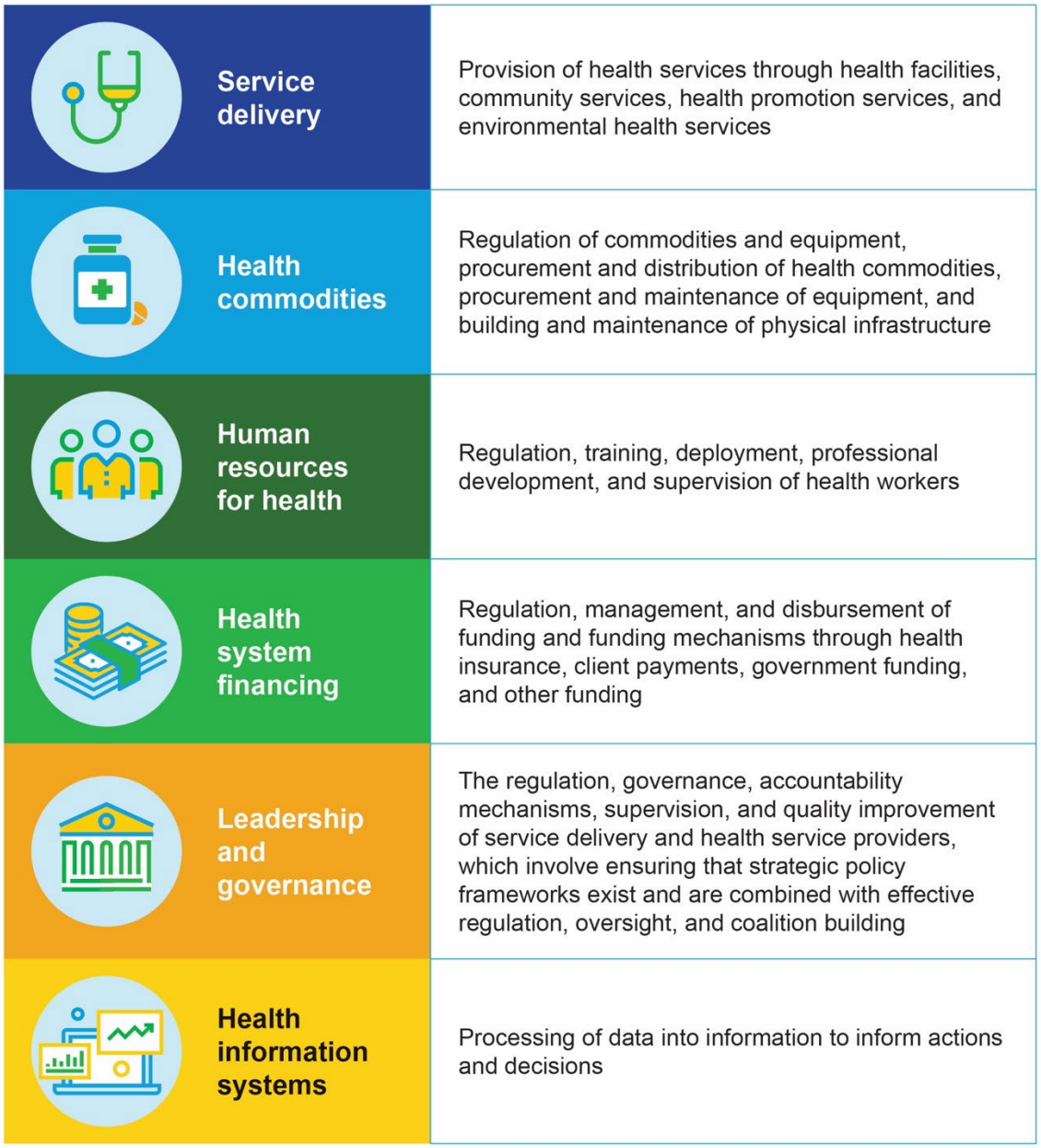
4.3 Tanzanian health sector

This section describes the building blocks and structure of the Tanzanian health sector.

4.3.1 Building blocks

The health system in Tanzania is organized according to WHO's health system building blocks (Figure 5).

Figure 5. World Health Organization health system building blocks.



Success of the TZHEA depends on, among other things, understanding clients' concerns across the six building blocks.

4.3.2 Health-sector structure

Management of health services in Tanzania falls under the GoT. The MoHCDGEC plays a stewardship role over the health sector, and PORALG plays a prominent role in implementation. Other ministries, departments, and agencies also have responsibilities related to the health sector. Certain private entities and nongovernmental organizations

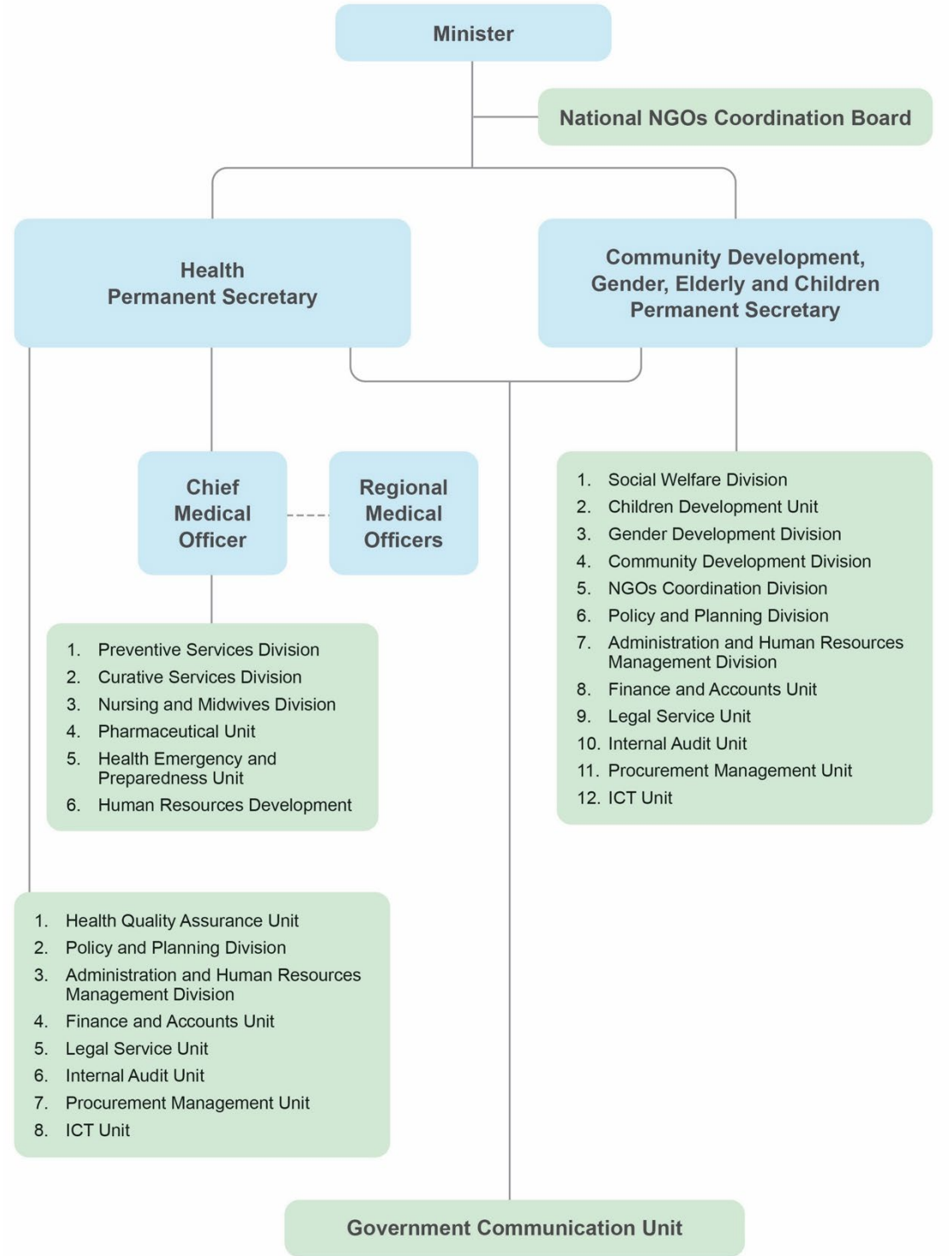
in the sector also play a role in service provision. Development and implementing partners provide financial and technical support. Citizens and communities also play a critical role in the health sector by accessing services, providing feedback, and holding service providers accountable. Within the health sector, sector-wide approach (SWAp) mechanisms are streamlined to serve joint planning, monitoring, and implementation of health-sector plans across different government and nongovernment institutions, through SWAp TWGs and the Joint Annual Health Sector Review.

4.3.2.1 MoHCDGEC

The MoHCDGEC is responsible for preparing health legislation and policies, as well as overseeing their implementation through sector-wide M&E. The ministry and its departments and agencies produce strategies, work plans, and guidelines to support legislation and policies that will ensure that all Tanzanians have access to high-quality health services.

Figure 6 depicts the MoHCDGEC leadership hierarchy, divisions, and units.

Figure 6. Functions and organizational structure of the MoHCDGEC.



Abbreviations: ICT, information and communication technology; MoHCDGEC, Ministry of Health, Community Development, Gender, Elderly and Children; NGO, nongovernmental organization.

The Preventive Services Division has several sections, including (i) Reproductive, Adolescent and Child Health; (ii) Environmental Health, Hygiene and Sanitation; (iii) Health Education and Promotion; (iv) Nutrition Services; and (v) Epidemiology and Disease Control. The Epidemiology and Disease Control Section oversees several programs, including the National AIDS Control Program, National Tuberculosis and Leprosy Program, National Malaria Control Program, National Onchocerciasis Control Program, Neglected Tropical Diseases Control Program, and eye care services.

The Curative Services Division has sections that include (i) Public and Private Health Services, (ii) Regional Referral Hospitals Services, (iii) Diagnostic and Health Care Technical Services, (iv) Traditional and Alternative Medicine, and (v) Non-Communicable Diseases, Mental Health and Oral Health.

The Policy and Planning Division has a section that coordinates all policy and planning issues, including health financing policy, and an M&E Section that coordinates health management information and M&E of health interventions.

The Pharmaceutical Unit is responsible for all aspects of health commodities, and the Human Resources Development Division is responsible for HRH. The ICT Unit coordinates digital health interventions.

4.3.2.2 Health regulatory authorities and agencies

A number of regulatory authorities and agencies fall under the MoHCDGEC, including:

1. ***Agencies:***

+ National Health Insurance Fund—provides health insurance.
+ MSD—is responsible for the supply of health commodities.
+ Tanzania Medicines and Medical Devices Authority—regulates quality and standards of health commodities, devices, and equipment.
+ National Blood Transfusion Service—collects and supplies blood products to health facilities.
+ National Institute for Medical Research—regulates, oversees, and performs health-related research.
+ Tanzania Food and Nutrition Centre—performs research related to food and nutrition.
+ Government Chemist Laboratory Authority—researches and regulates industrial consumer chemicals and human DNA.

2. ***Health facilities regulators:***

+ Private Health Accreditation Board—registers and regulates private health facilities.
+ Private Health Laboratories Board—registers and regulates private health laboratories.
+ Pharmacy Council—registers and regulates private pharmacies and accredited drug dispensing outlets.

3. ***Health worker regulators:***

+ Medical Council of Tanganyika—registers and regulates doctors.
+ Tanzania Nursing and Midwifery Council—registers and regulates nurses and midwives
+ Health Laboratory Practitioners' Council—registers and regulates laboratory professionals.
+ Pharmacy Council—registers and regulates pharmaceutical professionals.
+ Other health worker regulators, including the Optometry Council, Medical Radiology and Imaging Professionals Council, Environmental Health Practitioners Registration Council, and Traditional and Alternative Medicine Practitioners' Council.

4.3.2.3 PORALG

PORALG operates across sectors, including health, and oversees local government authorities (LGAs). LGAs establish and manage government-owned health facilities at or below the LGA (council) level, including allocating and supervising health workers; approving plans, budgets, and expenditures; and implementing health policies and guidelines. LGAs also supervise the quality of services provided by private and faith-based facilities within the council area.

4.3.2.4 Other government institutions

Other government institutions that are not entirely health focused play key roles in the health sector. They include:

1. ***President's Office–Public Service Management and Good Governance (POPSM&GG)***
   Is responsible for the management of government health workers, including in the health sector.

2. ***Prime Minister's Office (PMO)***
   Coordinates the work of all sector ministries, including the MoHCDGEC. The PMO includes two key health-sector organizations: the Tanzania Commission for

AIDS, which oversees the multisectoral HIV/AIDS response, and the Tanzania Social Action Fund, which provides financial social-protection services for the poorest, including linking them to health insurance.

3. ***Ministry of Finance and Planning (MoFP)***
   Plays a key role in managing and coordinating health financing. Entities under the Ministry of Finance and Planning include the National Audit Office, Controller and Auditor General, Tanzania Insurance Regulatory Authority, Social Security Regulatory Authority, and National Bureau of Statistics.

4. ***Ministry of Education, Science and Technology***
   Is responsible for managing and coordinating HRH training in institutions and universities. The ministry oversees the Tanzania Commission for Universities, which oversees universities; the National Council for Technical Education, which oversees technical courses, including technical pre-service training for health professionals; and the National Examinations Council of Tanzania, which manages secondary school examinations that are qualifying criteria for entry into training for health and other professions.

5. ***Ministry of Constitutional and Legal Affairs (MoCLA)***
   Manages and coordinates legal matters in Tanzania, including health-related ones. The ministry oversees the Registration Insolvency and Trusteeship Agency, which is responsible for the registration of birth and deaths—crucial information in the operations of the health sector.

6. ***Ministry of Home Affairs***
   Through the National Identification Authority, plays a key role in the provision of unique identifications for all Tanzanians, which is crucial to ensuring continuity of care in the health sector.

7. ***e-Government Authority (e-GA)***
   Is responsible for managing and regulating the implementation and use of ICT in GoT institutions.

4.3.2.5 Umbrella organizations and associations

Umbrella organizations and associations—including the Association of Private Health Facilities in Tanzania, which represents private health service providers; the National Muslim Council, which is officially known as Baraza Kuu la Waislamu Tanzania; and the Christian Social Services Council, which represents faith-based health service providers—play an important role by collaborating with the GoT.

4.4 Baseline business architecture

This section describes the stakeholders, challenges, and current business processes in which digital technologies can potentially play a role.

4.4.1 Service delivery

Service delivery in the health sector is tailored to support the overall objective of the *Health Sector Strategic Plan, July 2015–June 2020 (HSSP IV)*, which is to reach all households with essential health and social welfare services while meeting the expectations of the population, adhering to objective quality standards, and applying evidence-informed interventions through efficient channels of service delivery. Service delivery is the visible part of health care and the interface between the population and the health sector.

Table 3 describes stakeholders in the service delivery building block and their roles.

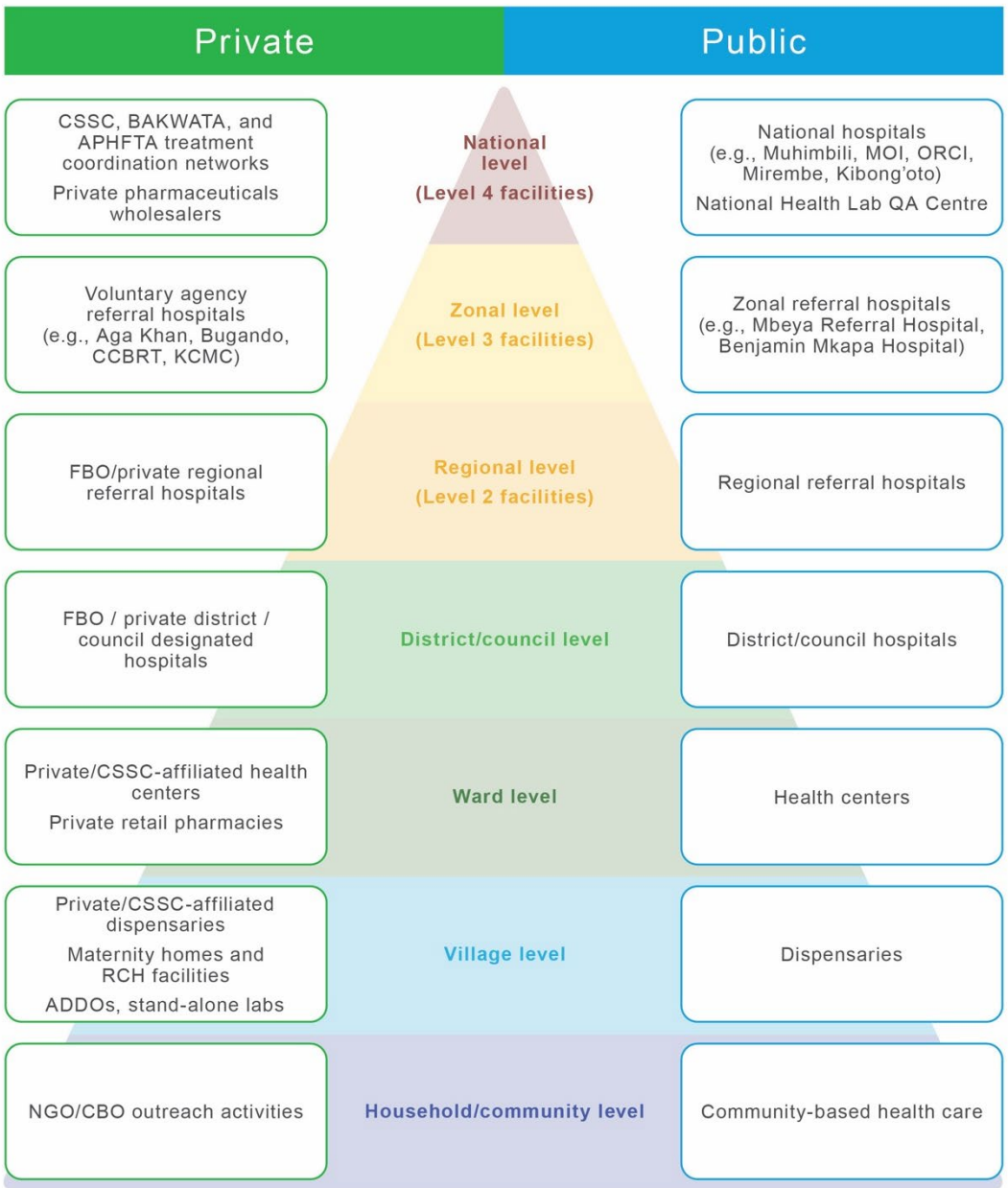
Table 3. Service delivery stakeholders and their roles.

Stakeholder	Role
Ministry of Health, Community Development, Gender, Elderly and Children	+ Formulates and reviews policies, regulations, and guidelines. + Oversees social welfare issues at the facility level; implements policies, guidelines, and standards. + Designs programs and interventions to address challenges in the sector that go beyond the capacity limits of local government authorities. + Sets strategic priorities related to service delivery; accredits health care facilities. + Implements national health promotion and education activities, including via media. + Implements national nutrition interventions, including food fortification, in collaboration with the Ministry of Agriculture.
President's Office–Regional Administration and Local Government	+ Oversees implementation of health policies and guidelines related to service delivery (health, social welfare, and nutrition services). + Oversees the development and implementation of health plans at the council level.
Regional secretariats	+ Coordinate and supervise service delivery.

Local government authorities	+ Supervise, plan, and manage service delivery. + Provide health promotion, nutrition, and environmental health services. + Oversee the work of community health volunteers. + Create a favorable environment for service delivery (by mobilizing resources, enacting bylaws, and motivating staff).
Health facilities	+ Dispensaries, health centers, and hospitals—provide preventive, rehabilitation, health promotion, and curative care services to clients. + Accredited drug dispensing outlets—dispense drugs and often provide basic health education to their customers. + Stand-alone health laboratories—provide health diagnostic services.
Ward health officers	+ Oversee and implement environmental health and sanitation interventions at ward level.
Community health service providers	+ Community health service providers, including community health volunteers, traditional and alternative health practitioners, and traditional birth attendants—support and link with the health services provided through health facilities.

Facility-based health services in Tanzania are delivered by government, faith-based, and privately owned facilities. Different health facilities offer services across different service delivery and management levels, as shown in Figure 7.

Figure 7. Categories of health facilities by service delivery level.



Abbreviations: ADDO = accredited drug dispensing outlet; APHFTA = Association of Private Health Facilities in Tanzania; BAKWATA = Baraza Kuu la Waislamu Tanzania; CBO = community-based organization; CCBRT = ; CSSC = Christian Social Services Council; FBO = faith-based organization; KCMC = ; MOI = Muhumbili Orthopedic Institute; National Health Lab QA Centre = National Health Laboratory Quality Assurance and Training Centre; NGO = nongovernmental organization; ORCI = Ocean Road Cancer Institute; RCH = reproductive and child health; CCBRT = Comprehensive Community-Based Rehabilitation in Tanzania; KCMC = Kilimanjaro Christian Center.

4.4.1.1 Service delivery business processes

Table 4 briefly describes the business processes that support health care service delivery at health facilities in Tanzania. All health facilities implement some or all of these processes, depending on the facility level.

Table 4. Business processes that support health care service delivery in Tanzania.

#	Process	Description
1	**Registration**	Process of identifying clients and recording or updating client demographic information, conducting triage, and taking vital signs to prepare client for consultation.
2	**Appointment**	An arrangement between a client and the health facility to book the date and time for accessing services.
3	**Client tracking**	Follow-up when a client does not turn up for scheduled appointments or when a client is found who is in need of services (e.g., case detection for diseases, identification of infants for immunization).
4	**Billing**	Mechanism for processing and accepting or waiving payment for services or health commodities (for both direct client payments and insurance claims).
5	**Consultation**	Assessment of client and provision of guidance and a course of action to improve the client's health.
6	**Investigation/ laboratory**	Diagnosis of the client's condition using laboratory services and tools, and provision of results.
7	**Dispensing**	Dispensing of health commodities, including medications and other items, to a client for use.
8	**Referral**	Redirection of a client from one point of service or facility to another for needed services that are not available at the current point of service.
9	**Inpatient department admission**	Monitoring and provision of health care services to a client who is staying in the facility for further interventions for a period of more than 24 hours.
10	**Radiology and imaging**	Diagnosis and reporting of a client's health condition using energy radiation and imaging tools.

11	**Electronic report submission**	Compilation, analysis, and transformation of client-level data into aggregate data for reporting, sharing, and use of individual client cases for surveillance purposes.
12	**Procedures and operations**	Performance of procedures or surgical operations on a client as part of treatment.
13	**Emergency**	Emergency response and provision of emergency care to client.
14	**Blood bank management**	Collection, storage, and distribution of safe blood.
15	**Mortuary**	Documentation of death, passing of information to relevant parties, proper handling of the body, and acquisition of lessons learned from the death.

Other service delivery processes take place outside the context of a health facility, including community health services, environmental and sanitation health services, nutrition services, and some non-facility-based health education and promotion services.

4.4.1.2 Service delivery challenges

The following challenges must be addressed to improve the quality of service delivery:

1. ***Inadequate adherence to guidelines and best practices***
   Inadequate adherence to clinical guidelines, protocols, standard operating procedures, and best practices by health care workers and service providers leads to unwanted client outcomes and misuse of resources.

2. ***Inadequate continuity of care***
   It is difficult to uniquely identify and track clients over time and across different service providers and delivery points.

3. ***Siloed services***
   The same clients often need different types of services, but some of these services are not integrated.

4. ***Inadequate client referral system***
   The referral system does not always operate smoothly due to factors such as inadequacies in transport logistics, communication, and feedback. The source of a referral does not usually request or receive any feedback from the referral destination on whether the referral was completed and what the outcome was.

5. ***Inadequate laboratory sample referral system***
   Management and tracking of test samples/specimens that are collected in one location and transported for testing to a laboratory at another location are delayed or inefficient.

6. ***Inadequate linkages to non-health services***
   Linkages between the health sector and other social services—such as birth and death registration, social welfare services, police and forensics, and legal services—do not always work efficiently and effectively.

7. ***Inadequate public awareness and health education***
   Limited public awareness of health problems and of the availability of different types of services leads to poor health behaviors, prevention, and self-management, as well as lower access to health care.

8. ***Inadequate availability of and access to services***
   Inadequate client access to services and particularly to specialized health services can be due to factors such as geographic remoteness, inadequate staff and resources at service provision points, lack of transportation, and out-of-pocket expenses.

4.4.2 Health commodities

Availability of health commodities at the point of care is critical for the delivery of high-quality services and client satisfaction.

Table 5 describes stakeholders in the health commodities building block and their roles.

Table 5. Health commodities stakeholders and their roles.

Stakeholder	Role
Ministry of Health, Community Development, Gender, Elderly and Children	+ Formulates policies, guidelines, and standards for health. + Supervises implementation and evaluation of policies, guidelines, and standards. + Performs and supervises the quantification and aggregation process (quantification, supply chain pipeline, and procurement plan).

Local government authorities	+ Plan and monitor the procurement process for health commodities, quantify health commodities, disburse certain commodities to facilities, provide technical supportive supervision to facilities, conduct medicine audit.
Health facilities	+ Quantify, procure (order and receive), store, manage inventory of, and dispense health commodities.
Medical Stores Department	+ Procures and stores health commodities; distributes some of them directly to health facilities and distributes some to LGAs for other vertical programs.
National Blood Transfusion Service	+ Coordinates blood transfusion and testing and supply of blood.
Private suppliers	+ Supply health commodities to (i) health facilities that normally procure from the MSD, when commodities are not available from the MSD; (ii) private health facilities that procure outside the MSD system; and (iii) accredited drug dispensing outlets.
Tanzania Medicines and Medical Devices Authority	+ Regulates safety, quality, and effectiveness of medicines, medical devices, and diagnostics in the health sector.
Tanzania Bureau of Standards	+ Undertakes measures for quality control of products of all descriptions and standardization of all products, including for health.

Abbreviations: LGA = local government authority; MSD = Medical Stores Department.

4.4.2.1 Health commodities business processes

Figures 8 and 9 show the key business processes in the health commodities supply chain.

Figure 8. High-level business processes at the service delivery point.

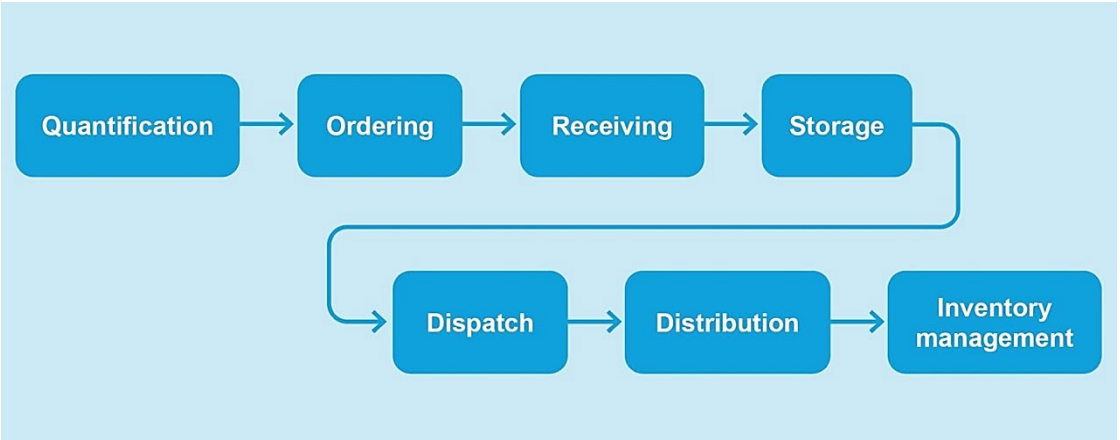
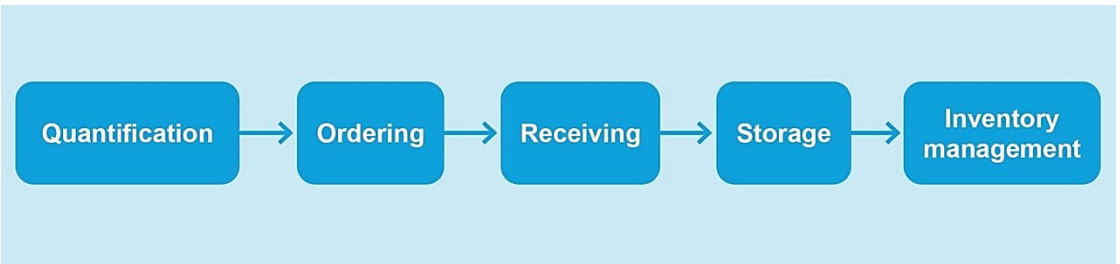


Figure 9. High-level business processes for health commodities suppliers.



4.4.2.2 Challenges in health commodities

The following challenges must be addressed to improve availability of health commodities:

1. ***Stockouts***
   Commodities stockouts are a major concern for the provision of high-quality health services to clients at health facilities. They may be caused by limited funding, improper quantification, or improper tracking of commodities.

2. ***Inadequate stock visibility***
   Visibility of stock availability within the facility (e.g., to prescribers, dispensers, and cashiers) and beyond the health facility (e.g., to the CHMT and the RHMTs) is inadequate.

3. ***Inaccurate forecasting and quantification***

Inaccurate forecasting and quantification of health commodities at health facilities may be due to inadequate forecasting and quantification skills and a lack of tools and accurate consumption data.

4. ***Insufficient visibility of stock availability at the MSD***
   Facilities order commodities without awareness of the availability at the MSD. Stockouts at the MSD are only noticed upon delivery and invoicing of commodities at the facility.

5. ***Inadequate inventory management***
   Management of stock across different areas of the facility where stock is stored and used is not effective. For instance, ledger and bin cards are not updated regularly or in a timely manner.

4.4.3 Health financing

Health financing focuses on ensuring that the health system has sufficient funds to deliver high-quality health services in an equitable way. Table 6 describes stakeholders in the health financing building block and their roles.

Table 6. Health financing stakeholders and their roles.

Stakeholder	Role
Ministry of Health, Community Development, Gender, Elderly and Children	+ Mobilizes and pools financial resources. + Sets health priorities and allocates funds for health-sector expenditures and grant mechanisms. + Regulates the price of health services. + Conducts health-sector expenditure review. + Formulates policies and guidelines on health financing, including insurance.
President's Office–Regional Administration and Local Government	+ Supervises allocated funds for service delivery at and below the LGA level. + Accounts for all expenditures and supports LGAs in identifying opportunities to expand their sources of revenue. + Coordinates preparation, scrutiny, and assessment of budgets. + Monitors and evaluates the implementation of approved budgets. + Coordinates partners working at the LGA level.

	+ Supervises implementation of policies, guidelines, and regulations at the LGA level.
Local government authorities	+ Support preparation, scrutiny, and assessment of health facility annual budgets. + Monitor and evaluate the implementation of approved budgets and annual plans. + Track facility expenditures. + Manage and control facility funds. + Contribute about 10 percent of council revenue to health facilities.
Health facilities	+ Prepare facility annual plans and budgets. + Purchase health commodities, equipment, and maintenance services. + Pay staff (in the case of private and faith-based facilities). + Collect user fees from clients. + Collect claims and capitation payments from health insurance providers. + Receive funds from the government and donors.
Ministry of Finance and Planning	+ Formulates, monitors, regulates, evaluates, and provides guidance on fiscal policies, guidelines, and standards. + Mobilizes and pools financial resources. + Supervises compliance with public and local government finance and public procurement legislation. + Allocates financial resources, sets annual budget ceilings, and disburses funds. + Administers public accounts. + Conducts public expenditure reviews. + Regulates insurers through the Tanzania Insurance Regulatory Authority.
Health insurance providers	+ Enroll clients in health insurance schemes (including National Health Insurance Fund schemes, CHFs, health insurance schemes of social security funds, and private health insurance schemes). + Collect regular insurance premiums from clients. + Invest funds collected in order to earn income. + Process and pay provider claims.

Development partners/implementing partners	+ Provide financial and technical implementation support.
Communities	+ Coordinate CHF enrollment in their community.
Social welfare	+ Provides health service user fee waiver to vulnerable groups.
Tanzania Social Action Fund	+ Supports enrollment of poor clients in CHFs.

Abbreviations: CHF = community health fund; LGA = local government authority.

4.4.3.1 Health-financing business processes

The business processes related to health financing include planning and budgeting, mobilization of funds, revenue collection, expenditure management, financial resource management, and provision of financial policy, laws, regulations, and guidelines.

Figure 10 shows the high-level businesses processes in health financing.

Figure 10. High-level business processes in health financing.

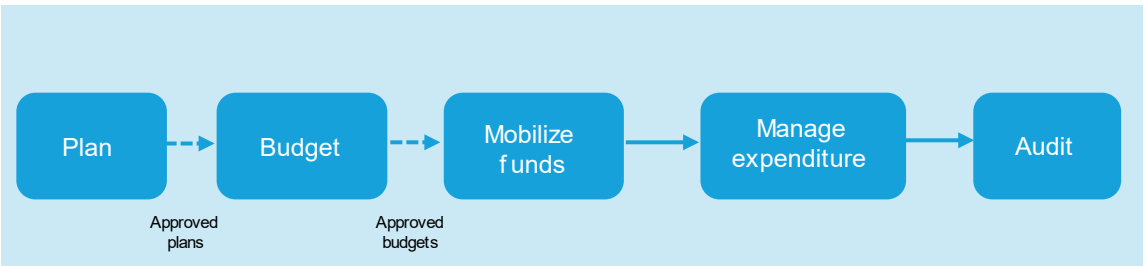
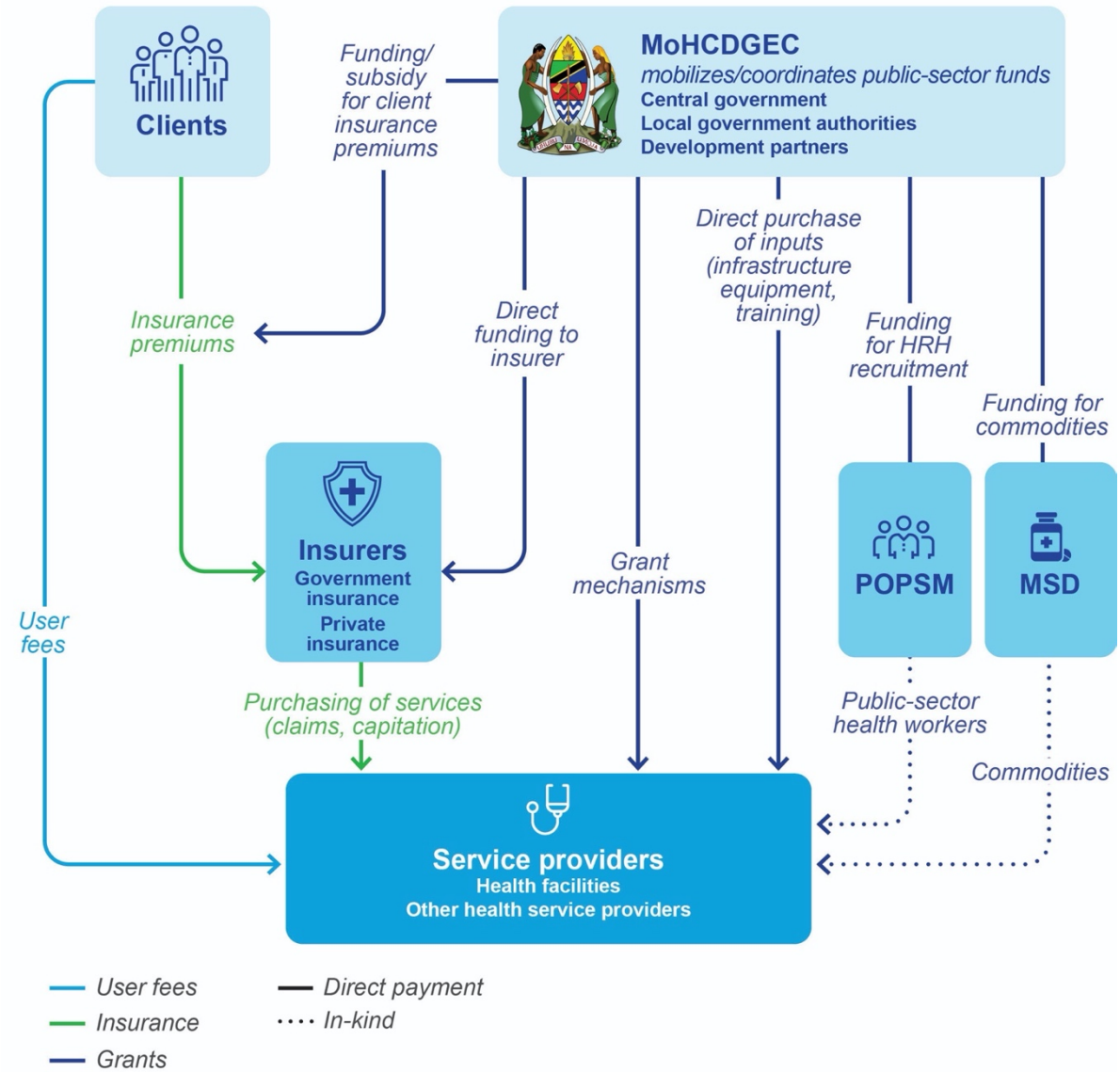


Figure 11 summarizes the movement of funds within the Tanzanian health sector.

Figure 11. Financing and payments across the Tanzanian health sector.



Abbreviations: HRH = human resources for health; MoHCDGEC = Ministry of Health, Community Development, Gender, Elderly and Children; MSD = Medical Stores Department; POPSM = President's Office–Public Service Management.

Funding and inputs for service provision ultimately come from clients and from public-sector funders, including government and development partners. Health service providers mobilize resources through different mechanisms:

1. ***Out-of-pocket payments***
   Clients may pay service providers directly for services.

2. ***Health insurance***
   Insurance may pay for services. Clients or their employers may pay their own insurance premiums, and the insurance premiums of the poorest people may be covered by mechanisms such as the Tanzania Social Action Fund. Government and development partners may provide subsidies or matching grants to insurance schemes. Service providers receive funds through claims or capitation processes.

   + Claims: Service providers are compensated for each service provided.
   + Capitation: Service providers are compensated based on the number of insurance clients who select their facility as one of their preferred facilities at the time of enrollment.

3. ***Grants and provision of inputs (such as human resources, commodities, and equipment)***
   These are transferred directly from government or development partners to service providers. The amount of the grant may be determined by budgetary processes or by schemes such as results-based financing.

4.4.3.2 Challenges in health financing

The following challenges must be addressed to improve health financing:

1. ***Non-universal insurance coverage***
   Enrollment in insurance is not universal, resulting in some clients not being able to access care for financial reasons and increased requests for waivers.

2. ***Non-recoupment of costs***
   Not all costs of services provided under exemptions, waivers, or subsidized prices are covered by government budgets, grants, and subsidies, resulting in financial challenges at health facilities.

3. ***Ineffective financial management***
   Planning, budgeting, accounting, and audit processes can sometimes have efficiency and effectiveness challenges, resulting in the risk of poor allocation or mismanagement of funds.

4. ***Limited financial resources***
   Limited financial resources and inequitable allocation of financial resources result in lower service quality.

5. ***Inadequate adherence to the insurance-claims payment process***

Inconsistences in documentation and claims processing lead to delays and/or rejection of claims. This affects facilities financially, limiting the financial resources they have for supporting service provision.

6. ***Nonstandard processes and procedures across insurance providers***
   Different insurance providers have different processes for identifying and verifying the eligibility of clients, and they require facilities to follow different processes and formats for submitting claims, which are not standardized.

4.4.4 Human resources for health

The GoT is strategically positioned to support three HRH capabilities: equitable distribution of health workers across the country, monitoring of health worker performance, and effective regulation of health workers. Delivery of high-quality health care and health services depends on the availability, knowledge, skills, and motivation of health workers.

Table 7 describes stakeholders in the HRH building block and their roles.

Table 7. Human resources for health stakeholders and their roles.

Stakeholder	Role
Ministry of Health, Community Development, Gender, Elderly and Children	+ Develops HRH policy and strategic plans. + Plans for and monitors the training and deployment of public- and private-sector health workers. + Ensures adequate and equitable distribution of HRH. + Approves placement of public-sector health workers and ensures a skill mix at service delivery points. + Oversees health professional regulatory councils and promotes ethical practices and conduct. + Strategizes on emerging new health challenges and the competencies needed to address them.
President's Office–Public Service Management and Good Governance	+ Manages public service, including public-sector health workers + Addresses civil servants' concerns. + Manages civil servants' data and information. + Monitors compliance with policies, circulars, guidelines, and standards for public service, good governance, and ethics.
President's Office–	+ Allocates public-sector health workers to LGAs. + Oversees implementation of HRH policy and strategy.

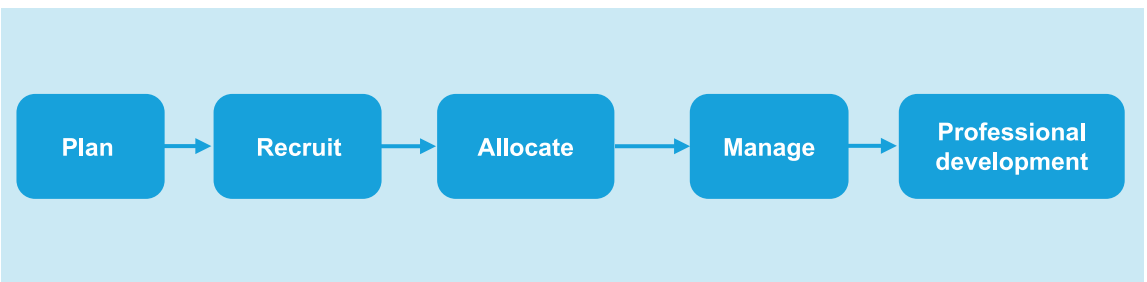
Regional Administration and Local Government	+ Oversees health worker welfare.
Local government authorities	+ Employ public health workers and allocate them to health facilities. + Implement HRH policy and strategy. + Oversee health worker welfare and performance. + Manage on-the-job training and CPD for health workers at and below the LGA level. + Process transfers, retirements, and exits for public-sector health workers.
Training institutions	+ Develop curriculum, teaching and learning resources, pre-service training, and examination and accreditation; coordinate internships, in-service training, and CPD.
Health professional regulatory councils	+ Register and accredit public- and private-sector health workers. + Manage ethics and competencies of health workers. + Ensure that public- and private-sector health workers are qualified and engaged in CPD.
Health facilities	+ Manage health workers' performance, on-the-job training, and CPD.

Abbreviations: CPD = continuing professional development; HRH = human resources for health; LGA = local government authority.

4.4.4.1 HRH business processes

Figure 12 depicts HRH business processes at a high level.

Figure 12. High-level human resources for health business processes.



4.4.4.2 HRH challenges

The following challenges must be addressed to improve HRH:

1. ***Shortage of skilled health workers***
   A shortage of skilled staff at health facilities results in, among other things, health care providers assuming multiple roles for which they are not fully trained. This creates risks and compromises the quality of health services offered.

2. ***Skewed distribution of skilled health workers***
   The available workforce is not equitably distributed, which affects the quality of the health services provided because the required professionals are not available in all places where they are needed.

3. ***Inadequate continuing professional development (CPD)***
   CPD is conducted in an ad hoc manner rather than in a coordinated and ongoing fashion that is tailored to health workers' needs.

4. ***Inadequate staff performance management***
   The performance management system for public-sector health workers—the Open Performance Review and Appraisal System—is ineffectively implemented, not fully operational, and unpopular among the administrators who are supposed to implement it.

5. ***Inadequate coordination of health workers across the public and private sectors***
   Public-sector health workers are managed by the POPSM&GG in the government HR system, but large numbers of health workers are not directly employed by the GoT; rather, they are employed by private or faith-based facilities, including facilities that have service agreements with the GoT. This leads to challenges in coordinating the distribution of health workers across the public and private sectors.

4.4.5 Leadership and governance

The processes involved in leadership and governance include policy formulation, planning and prioritization, client feedback, supervision of facilities and health workers, and M&E.

Various governance structures facilitate accountability, including health facility governing committees, Council Health Service Boards, CHMTs and RHMTs, and the Parliamentary Committee on Social Services and Community Development.

Service providers are directly accountable to the community and to the clients they serve. They are also accountable to government authorities and insurance providers, who in turn are accountable to communities and clients.

Tools used to facilitate governance and accountability include laws and regulations, policies and strategies, service agreements between LGAs and private health facilities, guidelines and standard operating procedures, M&E tools, community scorecards, client service charters, and supervision tools.

Table 8 describes stakeholders in the leadership and governance building block and their roles.

Table 8. Leadership and governance stakeholders and their roles.

Stakeholder	Role
Ministry of Health, Community Development, Gender, Elderly and Children	+ Formulates, disseminates, and oversees implementation and evaluates policies, guidelines, and standards related to health. + Establishes and institutionalizes governance structures.
President's Office–Regional Administration and Local Government	+ Oversees implementation of policies, guidelines, and standards related to health at the regional and council levels.
President's Office–Public Service Management and Good Governance	+ Approves administrative structures and establishes codes of ethics. + Oversees compliance with HR processes and issues standards, guidelines, and circulars on HR management and related issues.
Ministry of Finance and Planning	+ Formulates, disseminates, and oversees implementation and evaluates policies, guidelines, and standards related to finance in the health sector.

	+ Develops governance structures related to the finance sector that affect the health sector.
Ministry of Constitutional and Legal Affairs	+ Provides technical support in formulating acts and regulations related to health.
Local government authorities	+ Provide strategic direction, guidance, and priorities. + Supervise service providers and take disciplinary actions + Allocate resources. + Establish and monitor compliance with service agreements with health facilities. + Operate CHMTs and convene Council Health Service Boards.
Health facilities	+ Plan, set priorities for, and manage facility resources. + Monitor and evaluate health services provision. + Establish and comply with a client service charter.
National Audit Office of Tanzania	+ Controls and audits financial and nonfinancial resources, as well as financial governing systems.
Clients and communities	+ Hold service providers accountable. + Participate in health facility governing structures. + Identify health needs and participate in decision-making and priority setting. + Monitor service quality and provide feedback.

4.4.5.1 Leadership and governance challenges

The following challenges must be addressed to improve leadership and governance:

1. ***Inadequate supervision and performance management***
   Tracking of service provider performance is inefficient, as is coordination, continuity, and follow-up of supportive supervision and facility assessments.

2. ***Inadequate accountability***
   The use of tracking and measurement goals for service providers has not been effective.

3. ***Inadequate transparency and visibility***

Stakeholders—including the GoT, insurance providers, clients, and communities—do not have the information they need about the quality and quantity of service delivery to hold service providers accountable.

4. ***Inadequate policy implementation***
   Not all service providers and stakeholders adhere to policies and guidelines set out by the health sector's governing bodies.

4.4.6 Health Information

Sound and reliable information is a foundation for evidence-based decision-making across all health system building blocks. Such information is essential for health system policy development and implementation, governance and regulation, health research, HR development, health education and training, service delivery, and financing.

4.4.6.1 Health information business processes

The health information building block has four key data-related functions: (i) generation, (ii) compilation, (iii) analysis and synthesis, and (iv) communication and use. Data are generated from different sources; compiled; analyzed for their quality, relevance, and timeliness; and converted into information for evidence-based decision-making and action.

4.4.6.2 Health information challenges

The following challenges must be addressed to improve health information:

1. ***Unavailability and inaccessibility of information***
   Availability and access to information are insufficient for evidence-based decision-making and action.

2. ***Poor data quality***
   Siloed services and initiatives do not coordinate their data-generation tools and reporting forms, which leads to gaps and overlaps in data points and contributes to the poor quality of data.

3. ***Inadequate skills to transform data into information***
   Skills in analyzing and transforming data into information for evidence-based decision-making and action are lacking at all levels.

4. ***Unstructured change-management approach***
   The change-management approach for introducing and using digital solutions is not well defined or well implemented.

5. ***Inadequate support***
   ICT officers, usually one per district, are required to support ICT systems for all sectors, not just health, which makes it impossible for them to provide the required support to all health facilities in their district.

6. ***Disease- and program-specific solutions***
   Most HIS tools are developed to support the needs and business processes of a particular disease or program rather than focusing on health facility operations in a holistic manner.

4.5 Target business architecture

The target business architecture describes how the health sector should operate to achieve its vision, mission, and objectives.

4.5.1 Service delivery

The target architecture recommendations for service delivery are driven by the need for continuity of care, sharing of information, improved referrals, and effective client tracking.

It seeks to support the following capabilities:

1. ***Client experience***—accessible, convenient, time-saving, and efficient services for clients.

2. ***Quality of care***—improved quality and safety of health care services, including improved referral systems, more effective client tracking, and better adherence to standards, guidelines, and best practices.

3. ***Continuity of care***—better continuity of care within and across points of service, with appropriate sharing of client records and with follow-up over time

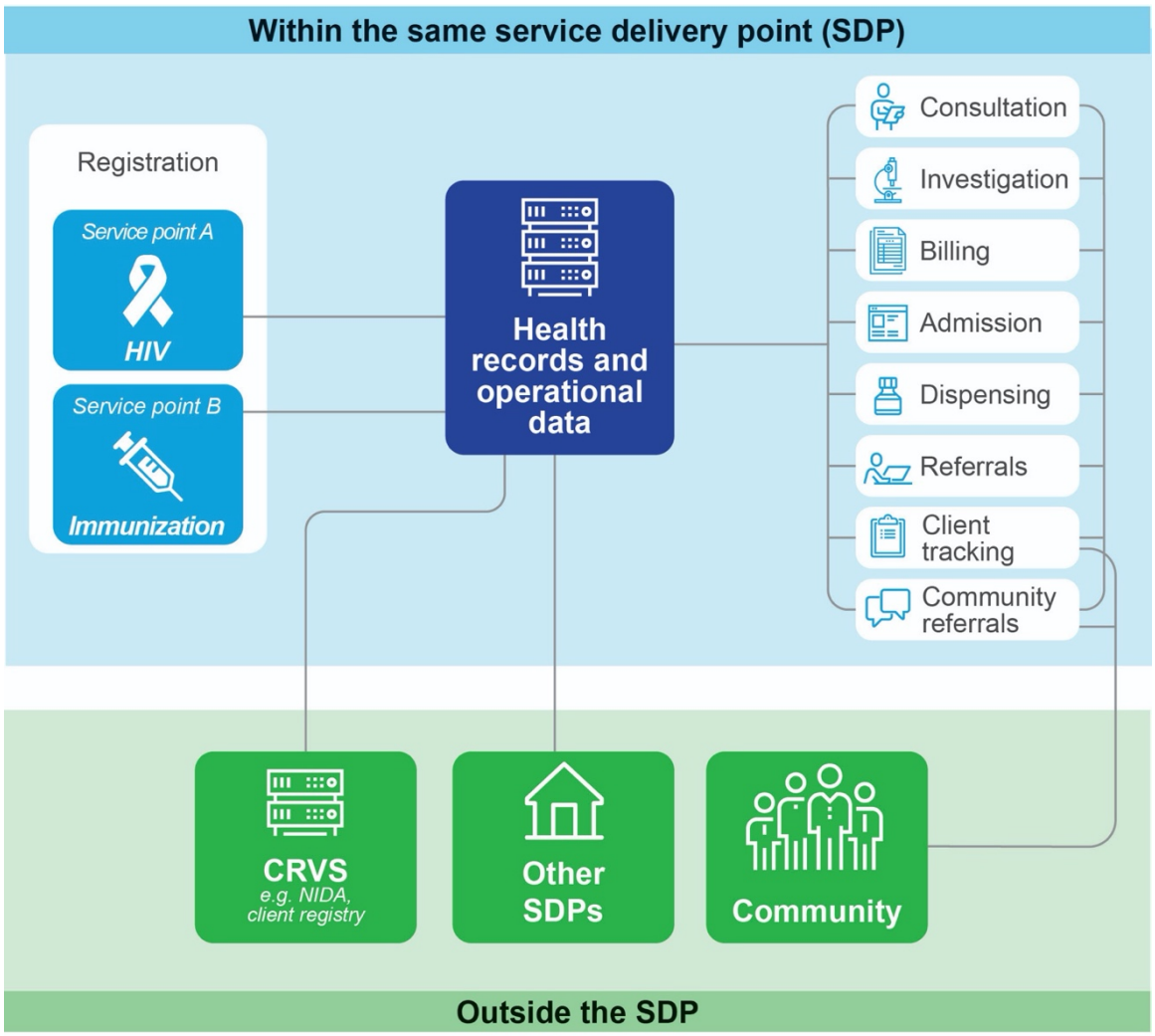
4. ***Integrated services***—better integration between different vertical programs and health services and between health and non-health services.

5. ***Communication with clients***—timely reminders, notifications, and educational messages to clients to keep them better informed.

6. ***Client access to services***—access for remote clients to expertise beyond what is available locally and to well-coordinated emergency transport services when needed.

Figure 13 shows recommendations for service delivery operations to promote better continuity of care.

Figure 13. How continuity of care can be achieved through improved service delivery operations.



Abbreviations: CRVS = civil registration and vital statistics; NIDA = National Identification Authority; SDP = service delivery point.

Table 9 describes how service delivery processes should operate to achieve better continuity of care.

Table 9. Recommendations on service delivery processes for better continuity of care.

Business process	Recommendations

Registration	+ Digitize the registration business process, with the option to have a connected and centralized data repository for all service points within the same facility and across facilities and service delivery points. + Provide a unique ID to all registered clients.
Consultation	+ Enable clinicians to access client records regardless of the facility from which the client previously obtained health services. + Provide digital tools that offer decision support to clinicians. + Allow facilities that are remote or have limited capacity to use telemedicine, in order to reduce the number of referrals to higher levels.
Investigation	+ Provide a linkage between the consultation and investigation to allow seamless transfer of test orders and results. + Enable records about lab specimens sent by a facility to another laboratory for testing to be communicated electronically to allow for notification and feedback between the referring facility and the laboratory. + Enable clinicians to have visibility into the types of investigation available in their facility.
Billing	+ Ensure proper documentation of all client bills at facilities, including clients on waiver. + Enable payments to be made electronically and be connected to the Government Electronic Payment Gateway.
Admission	+ Ensure documentation of services provided in the ward. + Ensure seamless linkage between the admissions department and other departments within the facility.
Community referral	+ Provide a mechanism to support referrals between community health service providers and health facilities.
Client tracking	+ Ensure continuity of care so clients who become lost to follow-up in longitudinal care programs are systematically identified and traced; provide mechanisms that distinguish between perceived and actual defaulters.
Reporting	+ When applicable, enable reporting to be done electronically, with the system generating the reports.

Dispensing	+ Provide linkages between prescription and dispensing data, as well as between consumption data and the services provided. + Improve visibility of the stock and of dispensed items both within and outside the service delivery point.

4.5.2 Health commodities

The target architecture recommendations for health commodities are driven by the need for availability and stock-level visibility of health commodities at all levels of SDPs.

The target architecture for health commodities seeks to support the following capabilities:

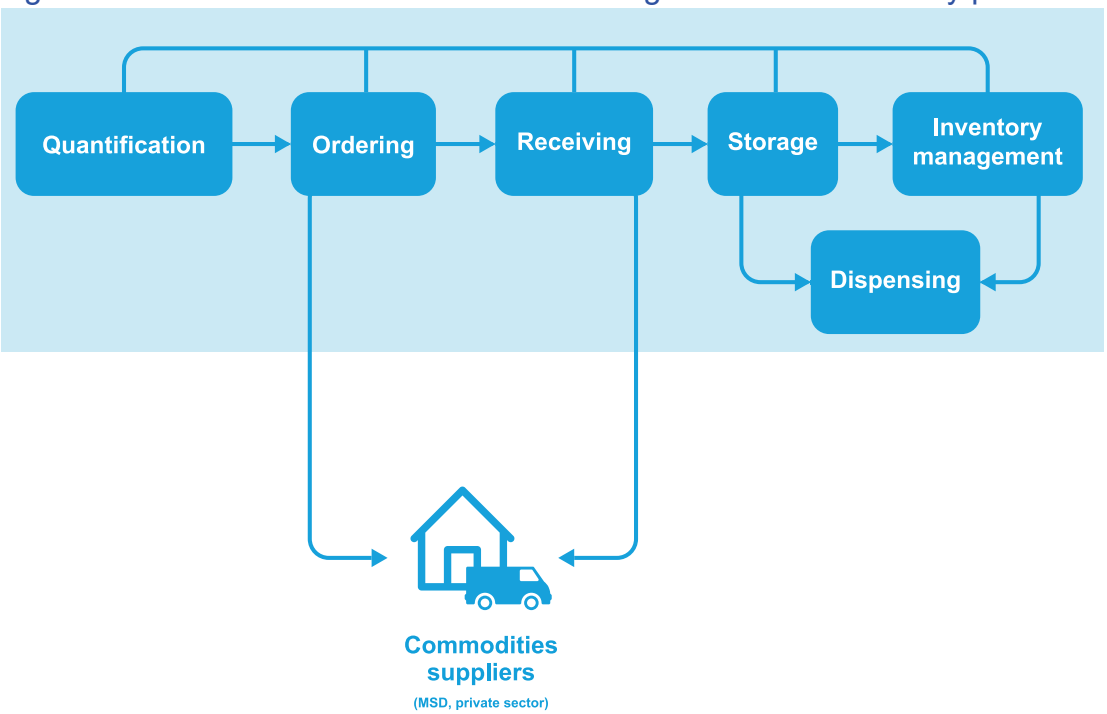
1. ***Improved governance and accountability***—improved governance and accountability throughout the health commodities supply chain through greater visibility and engagement.

2. ***Elimination of stockouts and pilferage***—improved procurement, supply, and inventory management to avoid stockouts and pilferage.

3. ***Information sharing***—increased access to health commodities information for different stakeholders, including LGAs, national-level leaders, and the MSD.

Figure 14 shows recommendations for managing health commodities at SDPs.

Figure 14. How health commodities are managed at service delivery points.



Abbreviation: MSD, Medical Stores Department.

The target architecture seeks to consolidate quantification, stock ordering, stock receiving, and storage as core aspects of inventory management, along with data on service delivery (such as drug dispensing). Inventory management will help identify stolen, expired, and broken commodities. Stock ordering and receiving will oversee incoming quantities of commodities.

Table 10 describes recommendations for managing health commodities.

Table 10. Recommendations for managing health commodities.

Business process	Recommendations
Quantification	+ Ensure proper documentation of consumption data that inform the quantification process. + Automate the quantification process using an electronic system that accounts for key factors (e.g., seasonality, previous consumption).

Ordering	+ Ensure that all relevant health workers within the facility have visibility into stock status and minimum reorder levels. + Ensure that ordering is done using a digital solution at the facility level.
Receiving	+ Enable facilities to receive notification of order fulfillment before the order arrives at the facility. + Ensure proper documentation of batch numbers to provide visibility into and track the expiration dates of health commodities.
Storage	+ Improve the mechanism for monitoring storage facilities for health commodities with special requirements, such as temperature-sensitive commodities. + Provide a mechanism to improve the visibility of health commodities stock at all levels.
Inventory management	+ Enable the inventory management process to be electronic and linked with consumption data from each relevant service provision point.
Equipment and infrastructure maintenance	+ Provide a mechanism to improve visibility of the status of equipment operations and maintenance. + Enable tracking of planned preventive maintenance of equipment.
Regulation of health commodities and equipment	+ Enable visibility of regulation status of health commodities and equipment.

4.5.3 Health financing

The target architecture recommendations for health financing are driven by the need for effective mobilization of resources and management of funds toward achieving universal health coverage.

The target architecture for health financing seeks to support the following capabilities:

1. ***Universal health coverage***—universal coverage with effective and efficient financial risk protection and coverage of essential health services, including clear processes and criteria for coverage of the poorest and most vulnerable

groups, such as through public financing for enrollment of these groups in insurance.

2. ***Effective recoupment of costs***—recouping of costs to facilities of subsidized services, waivers, and exemptions using sustainable and efficient mechanisms.

3. ***Efficient financial management***—use of mechanisms to improve adherence to financial regulations, rules, and procedures.

4. ***Access to financial information***—access for key stakeholders to relevant information about plans, budgets, funds mobilized, and expenditures, to enable better allocation of resources.

Figure 15 summarizes the target business processes for health financing.

Figure 15. Target business processes for health financing.

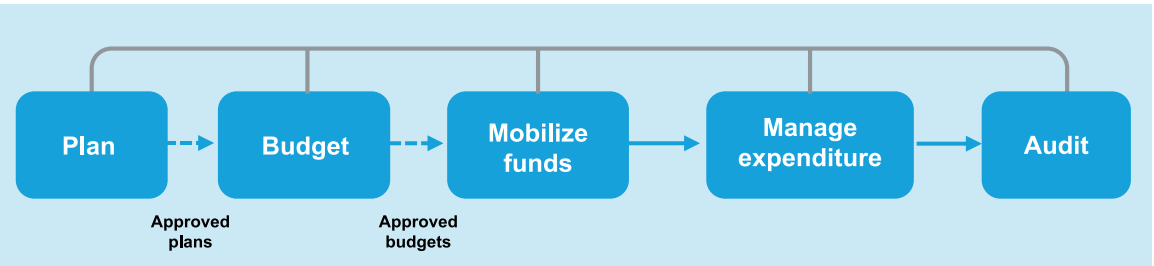


Table 11 describes recommendations for business processes for health financing.

Table 11. Recommendations for business processes for health financing.

Business process	Recommendations
Plan	+ Provide an electronic platform for managing plans (from lower-level service delivery points to the central government) and linking planning tools (such as between PlanRep and other digital health tools).
Budget	+ Ensure that the budget corresponds only to the plans outlined. + Make all changes to the requested budgets (e.g., rejections, approvals, budget cuts) available to all relevant stakeholders.

Mobilize funds	+ Align mobilized funds with plans and, where applicable, with specific budgets. + Facilitate universal health coverage through effective enrollment in insurance and mechanisms to support coverage of the poorest. + Provide efficient ways for service providers to recoup the costs of providing services and fund the services they provide through user fees, insurance claims and capitation, and government/donor grants.
Manage expenditure	+ Link all expenditures with plans, approved budgets, and sources of funding. + Make available a mechanism to provide information on expenditures and amounts allocated to avoid over- or underspending.
Audit	+ Ensure that the audit considers information about plans, budgets, and sources of funds for given expenditures.

4.5.4 Human resources for health

The target architecture recommendations for HRH are driven by the need for availability and equitable distribution of skilled health workers.

The target architecture for HRH seeks to support the following capabilities:

1. ***Equitable distribution of skilled health workers***—the ability of the health sector to manage and distribute available skilled health workers equitably.

2. ***Better management of skilled health workers***—efficient and proper mechanisms for managing, motivating, and supporting available skilled health workers.

3. ***Efficient CPD***—implementation of the CPD framework in a well-coordinated and well-regulated way.

Figure 16 summarizes proposed target business processes for HRH.

Figure 16. Target business processes for human resources for health.

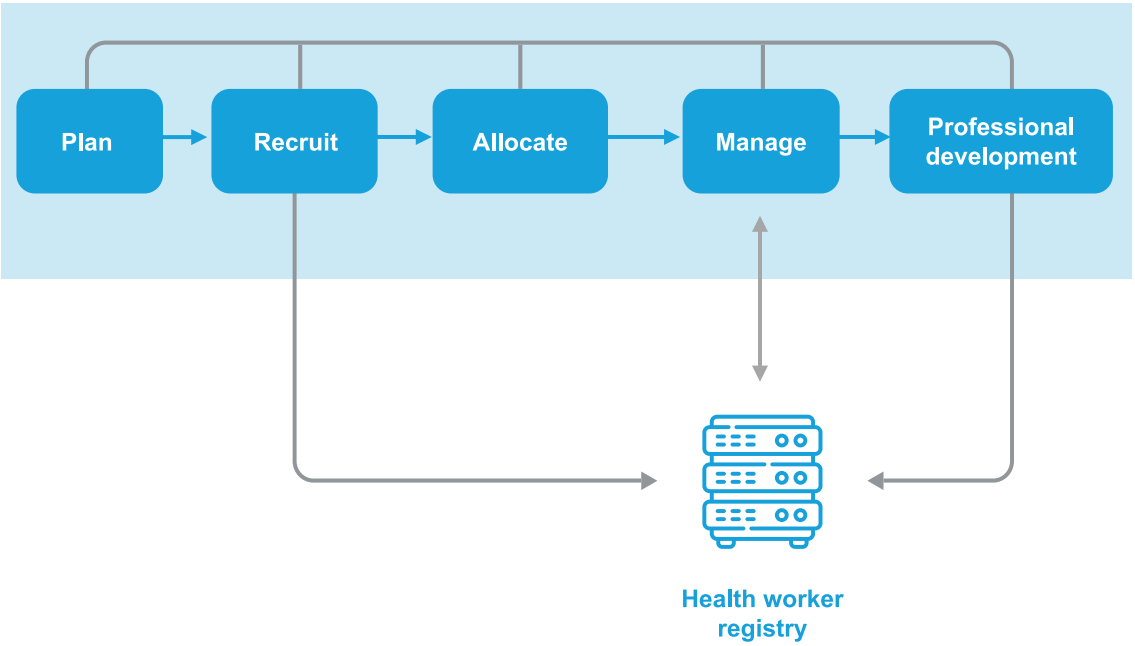


Table 12 describes recommendations for target business processes for HRH.

Table 12. Recommendations for business processes for human resources for health.

Business process	Recommendations
Plan	+ Enable better needs-driven allocation of health workers according to their cadre and skills.
Train	+ Align syllabus with identified needs, and train potential health workers in the required skills.
Recruit	+ Link recruitment for HRH with professional bodies to verify eligibility and qualifications of HRH staff.
Allocate	+ Ensure that allocation of staff is demand driven, by identifying places with the greatest need. + Provide a mechanism that enables visibility into the available health workforce in public and private facilities.
Manage	+ Make professional registration, registration renewal, and deregistration processes for public- and private-sector workers

	more efficient, and include more robust verification of qualifications and professional records. + Enable staff performance management systems to be more effective at monitoring, motivating, and supporting individual health worker performance.
Professional development	+ Provide a better link between HRH registration bodies, training institutions, CPD providers, and employers for coordinating professional development and tailoring it to individual health workers' needs over time.

Abbreviations: CPD = continuing professional development; HRH = human resources for health.

5 Data architecture

5.1 Introduction

A data architecture defines standards and models to govern how data are generated, used, stored, managed, and exchanged. In the health sector, it provides opportunities to simplify and standardize semantics and design data standards, achieve cost savings, and establish a more flexible foundation for supporting strategic business initiatives.[xii]

The data architecture for the health sector has the following objectives:

1. ***Outline existing datasets.***
   Document existing datasets, their life cycle, and their use within the health sector.

2. ***Improve data sharing.***
   Implement standards for accessing and sharing data within and beyond the health sector.

3. ***Improve data security and confidentiality.***
   Make recommendations for enhancing data security and confidentiality in health-sector ecosystems.

4. ***Establish data principles.***
   Define and document data principles that must be followed during planning, designing, and decision-making about data.

5. ***Establish common definitions of indicators.***
   Implement a data standard that facilitates harmonization and defines common indicators within the health sector.

5.2 Architecture principles

Data architecture principles should govern decision-making and planning about data.

Table 13 summarizes the data architecture principles.

Table 13. Data architecture principles.

Principle	Data as an asset
Reference code	TZHEA-D01
Statement	Data are assets and should be managed accordingly.
Rationale	+ To implement effective and careful data management, including ensuring where they reside, their accuracy, and their availability when required. + To make the correct information available at the right time and place so users can make the right decisions.
Implications	+ Manage information according to health-sector guidelines. + Provide decision support. + Make correct information available at the right time and place to support the right decision.
Principle	**Data as accessible and shared**
Reference code	TZHEA-D02
Statement	Stakeholders should have access to the relevant information according to their professional needs, responsibilities, and authority.
Rationale	To provide access to the correct information at the right time and place, which is critical for the quality and the efficiency of decision-making, to allow for both patient care and management.
Implications	+ Ensure that digital solutions comply with a common set of policies, procedures, and standards governing information accessibility and sharing. + Encourage all relevant stakeholders to participate in decisions on information management to realize health service goals. + Define the shared environment for information using standards and data models, data elements, and other metadata.

	+ Store metadata and make them available from a common repository. + Adhere to common policies when phasing out an old system in order to sustain access to necessary information. + Use common data models for the health sector to ensure the consistency of data. + Recognize that this principle may, in some cases, contradict information security requirements, but it should never lead to unintended disclosure of confidential information.
Principle	**Common terminology and data definitions**
Reference code	TZHEA-D03
Statement	Data should be defined coherently throughout the health sector, and definitions should be comprehensible and accessible to all users.
Rationale	+ To ensure that the data used in application development have common definitions so they can be shared. + To facilitate communication through use of common terminology and to promote efficient dialogue. + To share data and interfaces among different systems.
Implications	+ Establish common terminology for business activities in the health sector and use terms uniformly throughout the sector. + When a new data definition is required, coordinate and reconcile it with the health-sector data description “glossary.” + Address ambiguities arising from multiple data definitions by developing a definition that is accepted and understood by the entire sector.
Principle	**Data security and permissions**
Reference code	TZHEA-D04
Statement	Information sharing and disclosure of patient data should happen in accordance with relevant legislation and internal policies.

Rationale	+ To protect information from unauthorized access, use, or disclosure. + To make data available only to users who require the information as part of their role. + To balance the duty to protect and secure sensitive information with the duty to share and release public information.
Implications	+ Ensure that every person with access to patient-level data and information (both electronic and nonelectronic) adheres to the code of conduct for information security to prevent unauthenticated and unauthorized access to sensitive information. + Ensure that client data that should be available only in de-identified format are not re-identifiable. + Ensure that public policies and procedures for managing data confidentiality are followed. + Perform regular audits to ensure that access to information is based on professional need. + Identify and develop security needs at the data level, not the application level, in order to provide adequate access to open information while maintaining the security of sensitive information. + Include security in the design of data elements from the beginning; it cannot be added later. + Protect the system, data, and technologies from unauthorized access and manipulation.

5.3 Baseline data architecture

The baseline data architecture in the health sector describes how and where data are currently generated and how are they integrated, used, shared, and governed.

5.3.1 Data sources

The Tanzania HIS has two data sources (Figure 17):

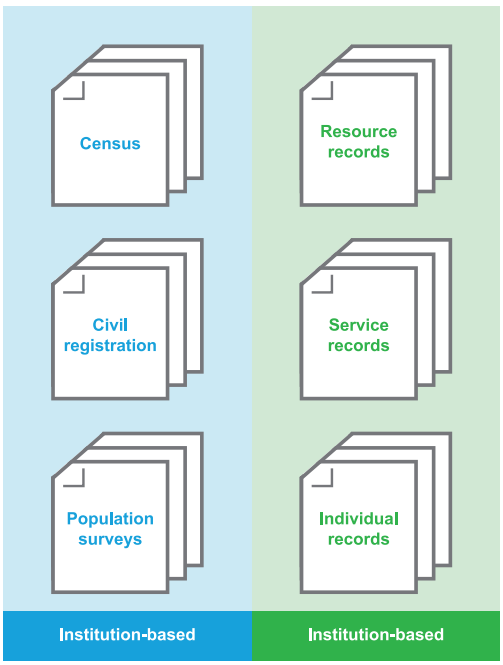
1. ***Institution-based data***
   These data, which include patient and facility records, are generated from administrative-based, facility-based, and community-based SDPs. The term *health institution–based data* refers to information created, collected, maintained,

transmitted, or recorded by an organization or establishment that was founded for the purpose of providing health-related services.

2. ***Population-based data***

These data are generated from a defined population and collected in either a continuous or a periodic manner. They include census data, vital statistics, household and budget survey data, and demographic surveillance data. The term *population-based data* implies that all information created, collected, transmitted, or recoded from all elements, individuals, or units meets the selection criteria in a particular area or place. In addition to the census, the major sources of population-based data in Tanzania are population health surveys, which provide nationally representative information on health status and access to health services.

Figure 17. Health information system data sources.



5.3.2 Data standards and guidelines

The e-GA has guidelines for developing data architecture and data standards for public institutions, but it has not defined specific data standards for the health sector to ensure seamless data exchange between systems and remove duplication of efforts, ambiguities, and inconsistencies in the use of data across the sector.

5.3.2.1 Data entities

No reference data entities have been defined for use in the health sector, so health-sector stakeholders define their own data entities. The e-GA guidelines recommend that all public institutions use international standards—such as from the International Organization for Standardization (ISO), World Wide Web Consortium (W3C), or Organization for the Advancement of Structured Information Standards (OASIS)—to define data entities.

5.3.2.2 Metadata standard

The e-GA has likewise not defined a health sector–specific metadata description. A standardized metadata description is critical to providing context for data assets. It allows the health sector to explain the origin, purpose, time reference, geographic location, creator, access conditions, and terms of use of a data resource.

The e-GA recommends that public institutions develop a metadata description based on the international Dublin Core™ model (ISO 15836) (Dublin Core is a trademark of the Dublin Core Metadata Initiative); this model provides the following standards for metadata and metadata element description:

- Dublin Core (Dublin Core Metadata Initiative Metadata Terms) standard—based on ISO 15836 and to be used for metadata description of websites, digital documents, and objects.
- Dublin Core Metadata Element Set—a simple and extensible metadata element set for facilitating discovery of electronic resources.

5.3.2.3 Data sharing

No standards for data sharing have been documented for the Tanzanian health sector, which leads to difficulty in sharing information among stakeholders.

5.3.2.4 Data life cycle

Different implementation levels have different data flows, which include stages where data are created, recorded, processed, reviewed, analyzed and reported, transferred, stored and retrieved, and monitored until retirement and disposal.

5.3.2.5 Security and confidentiality

The *Health Information System Guideline* provides guidance on data confidentiality and security, which states that confidential health information shall be defined as information that identifies an individual and relates to health information and comprises (i) past, present, or future health conditions; (ii) provision of health care to an individual; and/or

(iii) payment for health care. The guideline also provides guidance on the security and storage of electronic data, as well as of paper tools.

5.3.3 Challenges

Several challenges across the health sector's building blocks affect the quality of data collected and their use. The main challenges include:

1. ***Lack of coordination within the health sector***
   The HIS comprises separate vertical systems and components both inside and outside the MoHCDGEC. For example, disease-specific surveys are conducted in collaboration with development partners (e.g., the HIV/AIDS and Malaria Indicator Survey, Demographic and Health Survey, and the WHO STEPwise approach to Surveillance); population health surveys (including household budget surveys and the census) are managed by the National Bureau of Statistics, in collaboration with the MoHCDGEC and the Tanzania Commission for AIDS; the vital registration system (birth and death registration) is administered through the Ministry of Constitutional and Legal Affairs within the Registration Insolvency and Trusteeship Agency; and the resulting vital statistics are managed by the National Bureau of Statistics. Other information systems—such as for HR—logistics, and laboratory, are also managed by their respective sections or directorates. Efforts to improve data quality, such as conducting daily quality audits and assessments, are also uncoordinated across programs and can burden staff.

2. ***Inadequate terminology standardization***
   No common standards are in place for diagnosis, diseases, and financial data across the health sector. For example, standards such as the *International Classification of Diseases, Tenth Revision* (ICD-10), are recommended, but they are not widely used in the health sector. Likewise, no standards for health commodities are in place for distribution and storage processes, prescription processes, and dispensing processes, making tracking of commodities difficult.

3. ***Manual data processing***
   The paper-based nature of the system increases the chance of human error when transferring data from paper registers to tally and summary sheets and then into the District Health Information System.

4. ***Existence of multiple data tools***
   Health service providers are required to use different data tools containing similar information. The multiple, proliferating, and unconnected data systems lead to an increased burden on health facility workers.

5. ***Unavailability of data management staff***

   Most health facilities do not have designated data management staff, so clinical staff must take extra time to complete numerous forms. The staff are often not adequately trained on the systems, which compromises the quality of the data.

6. ***Inadequate management of public- and private-sector health worker data***

   Public health worker records are maintained by the POPSM&GG, but similar data for the private sector are not available. Health worker data are available in various health worker regulatory council databases, but these data are not easily analyzable as a whole. The HRH Information System aims to maintain data on both public and private health workers, but the information flows are not well established, leading to data gaps.

7. ***Inefficient data sharing between training institutions and regulatory councils***

   Health workers must present qualifications, training credentials, and CPD information to regulatory councils in order to register and renew their registration. However, this data flow is not streamlined in many cases, leading to delays and risks of certificate forgeries.

8. ***Inadequate data on health worker training and CPD***

   Information regarding CPD for health workers is fragmented, which makes it hard to support data-driven planning and decision-making.

9. ***Inadequate data security and confidentiality***

   Most confidential health data are held in health facilities in paper-based registers, where the risk of access by unauthorized individuals is relatively low. However, Tanzania is quickly moving to a system of electronic health records. While there are potentially negative consequences to clients if their confidential health information is accessed in its current paper-based format, the risks are greater when all health information is available in an electronic system. No specific law is currently in place to protect personal health data in Tanzania, although various laws exist to safeguard protected data.

10. ***Inadequate data analysis skills, data dissemination, and data use***

    The health sector has inadequate capacity for data analysis, interpretation, dissemination, and use to inform regional, council, and facility performance. Inadequate attention is given to data analysis, dissemination, and use, which hampers evidence-based decision-making, resource planning, and policymaking. Most facilities lack computers and do not have access to their own data entered into the District Health Information System.

5.4 Target data architecture

The target data architecture sets standards and guidelines to support the health sector in meeting its vision, mission, and objectives.

The target data architecture seeks to support the following capabilities:

1. ***Improved data sharing and integration***—use of standards for data and metadata definition for data sharing between stakeholders and systems.
2. ***Unified reporting***—use of predefined datasets and standards, allowing data from SDPs at different levels to be easily aggregated for reporting.
3. ***Shortened data processing time***—use of predefined standards and formats, reducing the amount of time required to process data before analysis and for decision-making.
4. ***Improved availability of high-quality data***—guidelines and recommendations that facilitate the availability of data at different administrative and operational levels.
5. ***Common reference of core datasets***—availability of core datasets, which help different stakeholders have a common reference to data regardless of where they were generated.

5.4.1 Standards and guidelines

This section outlines recommended standards for the target data architecture, including standards for data element sets, metadata documentation, coding, and security and confidentiality. Data standards enable information sharing and workflow participation from different institutions and applications. Common standards are important for integration, interoperability, and scalability, as well as for the quality of services. Standards help prevent ambiguity and inaccuracies in the information exchanged, which can result in risks to patient safety, quality of care, and resource management.

5.4.1.1 Data entities

Table 14 summarizes the recommended data entities for the health sector.

Table 14. Recommended data entities for the health sector.

Data entity	Description	Basic data elements

Client	Information allowing identification of a client (any recipient of health care services)	Client identification number, first name, second name, last name, date of birth, gender, nationality, residential address, relationship links between clients (e.g., parent-child)
Health worker	Information about a person who provides health care services	Health worker name, national identification number, cadre, training, qualifications, assessments, performance evaluations
Health facility	Information about a health facility or service delivery point	Identification number, name, location, type, services provided, ownership, operational status, date opened, status
Admission	Information related to the admission and discharge of the client during an inpatient visit	Admission date and time, admission type, bed/ward allocation, discharge date and time, discharge type
Diagnosis	Process of reaching a conclusion (diagnosis) by determining which disease or condition is affecting human health	Health condition type, diagnosis name, diagnosis code
Observations and triage	Observations made by the health worker during the course of examination and discussion with the client, including vital signs to assess the most basic body functions—applicable during an outpatient visit or continuously during an in-patient admission	Temperature, blood pressure, swelling, stable versus critical condition
Birth	Information about a birth	Date of birth, birth type
Death	Information about a death	Date of death, cause of death

Order	Information about an order to provide a service, including for diagnostics and tests, procedures, and commodities (prescription)	Order date, service/item ordered, ordering health worker, quantities and dosage, route
Investigation	Information about laboratory tests, imaging, and other diagnostics	Investigation type, sample status, time collected, result
Procedure	Course of action intended to achieve a result for the person with a health problem; information about the procedure or operation, including anesthetic information	Procedure name, procedure code
Referral	Information related to the referral of the client	Incident date, referral type, referral source, referral destination, reason for referral
Appointment	Information on individual appointments and on schedules of care	Appointment date, appointment type, type of service
Client tracking	Information related to client tracking	Tracking method, tracking status, tracking outcome (lost, transferred, died, opted out)
Commodity	Health commodity type	Commodity name, commodity code, commodity description, expiration date, batch number
Equipment	Types of physical, non-consumable items that are used during the care of a client	Equipment name, equipment number, manufacturer, equipment code, maintenance date, operational status
Inventory	Information about stocks and flows of commodities, including dispensing	Order, delivery, storage location, dispensing, expiration, damage, physical counts, collection (for blood products)
Insurance	Information about a client's enrollment in insurance and eligibility for coverage	Membership number, covered services, enrollment date, expiration date

Billing	Data elements that are related to billing for out-of-pocket or insurance purposes; waiver information	Bill ID, bill type, bill amount, bill item, bill service, waiver decision, submitted claim, verified claim, paid claim, payment method, payment control number
Expenditure	Information about expenditures, including budgets, expenditure amounts, and audits	Expenditure amounts, dates, services, approvals, audit status

5.4.1.2 Metadata documentation

Table 15 provides an example of a data element list with recommended minimum metadata documentation.

Table 15. Example data element list with minimum metadata documentation.

#	Item	Description
1	**Name**	Name of the data element.
2	**Code/ID**	The reference code/ID for a data element adopted from a known standard (e.g., *International Classification of Diseases, Tenth Revision*).
3	**Description**	A simple and unambiguous definition of a Generic or Custom data element.
4	**Type**	+ Generic: a commonly used data element across different applications in the health sector. + Custom: used in a particular application only.
5	**Is part of**	Description of the main data entity/element that this data element is part of.
6	**Parts, if any**	Description of the parts of a variable (e.g., first name, second name, and surname in the name data element).
7	**Data format**	Format such as Varchar, Character, or Decimal for real/floating numbers; Integer for whole numbers; or Date The recommended style of printing/display, if required.
8	**Maximum size**	Maximum size of the data element.

9	Validations	Generic validations for generic data and specific validations for custom data to be applied for acceptance of data.
10	Values	List of Acceptable Values.
11	Values code/ID	A reference code/ID for the value of a data element adopted from a known standard.
12	Default value	A default value/input that should be used if no value is supplied.
13	Owner	Name(s) of the department(s) and/or role(s) that own the data element or Code Directory and have updating rights.
14	Based on	Reference to the document/standard to which the data element is standardized.
15	Version	Version number of the data element.
16	Status	Current status of the standard (draft or accepted).
17	Date agreed	The date on which this version of the standard was accepted.
18	Verification	Steps taken to establish the correctness of Generic or Custom data elements at different levels.
19	Comments	Additional notes, if any.
20	Date of publishing	The date on which the standard was published or a PDF version was created.
21	Example/ illustration	A suitable sample data element to be used as a reference for its use.

Table 16 provides an example of a metadata description for the date data element.

Table 16. Example metadata description for the date data element.

#	Data element	Metadata description
1	Name	Date
2	Code/ID	Not applicable

3	**Description**	Date as per e-Government Authority date conventions (dd/mm/yyyy)
4	**Type**	Generic
5	**Is part of**	Not applicable
6	**Parts, if any**	Day Month Year
7	**Data format**	Date (dd/mm/yyyy)
8	**Maximum size**	10 (dd/mm/yyyy)
9	**Validation**	+ **yyyy:** a valid year in four digits. + **mm:** in the range of 01–12. + **dd:** in the range of 01–31 but not greater than 30 in April, June, September, and November; not greater than 31 in January, March, May, July, August, October, and December; and not greater than 28 in February, except in a leap year, when a value of 29 is allowed.
10	**Values**	Per allowable ranges on validation
12	**Default value**	Not applicable*
13	**Owner**	Not applicable**
14	**Based on**	As per e-Government Authority standards
15	**Version**	Not applicable***
16	**Status**	Accepted
17	**Date agreed**	Not applicable****
18	**Verification**	Not applicable*****
19	**Comments**	“/” to be used as a delimiter for the representation of a date
20	**Date of publication**	16/11/2011

21	Example	10/01/2017 for 10 January 2017

** Some date variables may have default values, depending on the reason for capture.*
*** May be documented if a variable can be modified only based on guidelines from a certain organization and/or standard.*
**** May be documented if the data source keeps track of versions and approvals of data elements.*
***** May be documented to capture the date of the approved version.*
****** May be documented if inputs for the given data element should be verified against inputs from other data elements and/or a predefined range (e.g., a data element for capturing pregnancy may be verified against the gender data element to ensure that male clients cannot be registered as pregnant).*

5.4.1.3 Coding standards

Table 17 shows the recommended standards to facilitate data sharing.

Table 17. Recommended standards to facilitate data sharing.

Standard	Description	Recommendations
International Classification of Diseases (ICD)	A statistical classification system for assigning diagnostic and procedural codes in order to produce coded data for statistical analysis, epidemiology, reimbursement, and resource allocation	All health data systems should use ICD coding for disease specification.
Logical Observation Identification Names and Codes (LOINC)	A universal code for identifying laboratory measurements and clinical observations	Health systems should use LOINC to define laboratory measurements and clinical observation.
Systematized Nomenclature of Medicine-Clinical Terms (SNOMED CT)	A clinical terminology for capturing and representing patient data for clinical purposes	The system should use this standardized terminology.

Abbreviations: ICD = International Classification of Diseases; LOINC = Logical Observation Identification Names and Codes.

Table 18 describes recommended security principles for data protection and management.

Table 18. Recommended security principles for data protection and management.

Principle	Description
Authentication	Use of a password or combination of tokens, biometrics, or multiple authentications to control access to health information.
Authorization	Use of role-based access controls.
Encryption	Rendering shared health data and information unreadable until they are decrypted by an authorized user.
Integrity	Assurance that health data and information are protected from unauthorized alteration and destruction, whether accidentally or deliberately, and that information and programs are changed only in a specified and authorized manner.
Accountability	Ability to track and monitor activities associated with the access and use of eHealth systems (interactive and automated, messaging and online).
Assurance and awareness	Ability to ensure that (i) existing health data and information are of high quality, (ii) monitoring and evaluation tools and procedures are in place for identifying data quality issues that need to be addressed at each level, and (iii) user education is continuous to ensure that key officials, stakeholders, and service providers are aware of the enterprise architecture vision, goals, and principles.
Auditing	Required tracking of all changes in access to information and all changes to data and information.

5.4.2 Data flow and data sharing use cases

Table 19 provides use cases to illustrate data flows and data sharing.

Table 19. Data flow and data sharing use cases.

Building block	Type of information	Use case
Service delivery	Client health data	+ Between different points of service within a health facility. + Between one health facility and another.

		+ Between health facilities and community service providers.
	Orders (e.g., diagnostics orders, prescriptions)	Between different points of service within a health facility and between health facilities.
Health commodities	Authenticity data	Between health facilities, regulators, and clients.
	Orders	From health facilities to suppliers.
	Supply	Between health facilities and suppliers.
Health financing	Client insurance enrollment verification	From insurers to health facilities.
	Insurance claims	From service providers to insurers.
	Budgets, plans, revenues, and expenditures	Between service providers and decision-makers.
Human resources	Qualification, training, and CPD status	Between training institutions and CPD providers and health worker regulators.
	Health worker registration information	Between health worker regulators and employers (including the POPSM&GG as a health worker employer).
Health information systems	Aggregated service delivery information	From service providers to government decision-makers.
	Public health events, such as for immediately notifiable disease cases and disasters	From service providers to government decision-makers.
Leadership and governance	Facility supervision and assessment information	From supervisors to facilities and government decision-makers.
	Client feedback	From clients to service providers.
	Facility information on service availability, commodity stocks, services provided,	From service providers to clients and facility governing structures.

	revenue, and expenditure	

Abbreviations: CPD = continuing professional development; POPSM&GG = President's Office–Public Service Management and Good Governance.

5.5 Gap analysis and recommendations

5.5.1 General gaps and recommendations

Table 20 describes gaps in the baseline architecture and offers recommendations for supporting better operations in the health sector.

Table 20. Gaps in the baseline data architecture and corresponding recommendations.

#	Baseline gap	Recommendations
1	**Reference data repositories**	Reference repositories should be used consistently across the health sector to allow for better data exchanges and integration. For example, having a shared administrative area registry will allow for consistent integration of data within the same areas, and a centralized service delivery point repository will allow for better allocation of staff and planning of interventions (for services reported by each standardized service delivery point).
2	**Reference data and metadata dictionary**	A reference data and metadata dictionary should be used to define common data variables and process them across the health sector. For example, a standard date format, name format (first name, second name, and surname), allowable personal IDs, etc. will enable easy integration of data across different platforms.
3	**Data-sharing standards**	Data-sharing standards should be used to guide the processes and data manipulations required to move data from one platform to another.
4	**Data aggregation standards**	Data aggregation standards should be used to guide how data from the individual level should be processed for reporting in an aggregate manner. Such standards

		allow for unified reporting of aggregated data across the health sector. They may cover recommended age categories/groups, geographical coverages, etc.
5	**Data security and confidentiality standards**	Health-sector data security and confidentiality standards should be used to guide how data should be collected, stored, processed, and exchanged, while ensuring that the processes are secure and client privacy is protected.
6	**Individual-level health records**	Individual-level health records will have all the data needed for processing, analysis, and reporting, if required, and allow for more flexible analysis.
7	**Data modeling and business intelligence tools**	The centralized data warehouses should be linked to data modeling and business intelligence tools to enable better trends analysis and automated guidance on planning and actions. Outputs from these tools should be made accessible to key stakeholders, including decision-makers at the central government and local government authority levels.
8	**Data security strategies, policies, and guidelines**	Well-documented data security strategies, policies, and guidelines should guide what happens at different implementation levels.

5.5.2 Gap analysis and recommendations by building block

Table 21 describes the baseline gaps and offers recommendations for each building block.

Table 21. Baseline gaps and corresponding recommendations for each building block.

#	Baseline gap	Recommendations
Service delivery		
1	**Multiple client registration points at the same SDP, leading to duplicative work**	Client demographic data collected and/or updated at different registration points within the same facility should be made available at all points. Individual clients should not have multiple registration records.

2	**Inadequate linkage between registration at health facilities and other institutions that do client registration, such as NIDA and RITA**	Client registration data should be linked with other institutions that do client registration outside the SDP, for verification and/or submission purposes (e.g., births and deaths).
3	**Lack of sharing of client medical records between departments within the same SDP**	All departments within the same SDP should have access to all relevant medical records for their operations.
4	**Inability to share client medical records across SDPs**	Without jeopardizing client privacy and confidentiality, relevant client health records should be accessible to other SDPs to allow for continuity of care.
5	**Use of multiple tools to record client medical records leading to different sources of reporting information**	Service delivery records should be stored using a tool that ensures continuity of service within and outside the facility and a single data compilation site.
Health commodities		
1	**Lack of visibility of SDP inventory and logistics information**	SDPs should be able to update stock information as commodities are consumed. Updates to stock records should be made accessible to all relevant parties.
2	**Quantification process informed by low-quality data**	An SDP's quantification process should use data on health commodities usage (e.g., dispensing).
3	**Inadequate visibility of stock availability at the MSD during ordering and while orders are in the pipeline**	SDPs should have visibility into the availability of health commodities on order before an order is delivered to allow for planning of alternative procurement.

4	**Lack of visibility of health commodities management data at all levels (i.e., council, regional, and national)**	Health commodities management data from SDPs should be made available to LGAs and at the national level. This should include quantification, ordering, receiving, and usage data (available stock, dispensing, damage, expirations, etc.).
Human resources for health		
1	**Inadequate linkage of HRH staff registration data and recruitment, management, and professional development processes**	Recruitment of HRH staff should be informed by data in the health worker registry. HRH registration details should also inform and/or be updated as part of HRH staff management (e.g., deaths, professional development information).
2	**Inadequate linkage between HRH staff allocation and staff management processes (e.g., transfers and retirement)**	Allocation of new staff should be informed by the latest HRH records at different SDPs. This should include allocation guided by transfers, deaths, retirement, etc.
Health financing		
1	**Inadequate records of clients served on waiver**	To allow for proper estimates of the funding spent by SDPs on clients on the waiver program, payment systems should capture records of services offered to those clients.
2	**Inadequately centralized management and allocation of mobilized resources**	To allow for better resource use, management of resources allocated to different interventions and locations should be centralized. Shared information should be made accessible to all relevant stakeholders.
3	**Inaccessibility of relevant financing records to stakeholders outside of SDPs, up to the national level**	Data storage should be centralized and include all financing records, which should then be accessible to stakeholders at all levels.
Leadership and governance		

1	**Inadequate mechanism for managing stakeholders**	Centralized data storage with a record of stakeholders, levels of engagement, coverage areas, etc. should be used. Better documentation of stakeholder engagement will improve stakeholder management.
2	**Inadequate tracking of M&E outcomes**	Centralized data storage should be used to facilitate documentation of M&E activities, including observations, follow-ups, and outcomes.
Health information systems		
1	**Inadequate mechanism for tool review and approval**	All national-level tools for collecting and/or generating data should be reviewed before they are used at SDPs to avoid duplications and ensure adherence to standards.
2	**Inadequate data use and visibility at all levels**	A mechanism for data visibility to inform the decision-making at all levels should be used.
3	**Data tool design**	Data tools, whether paper or electronic, should be designed primarily as job aids to facilitate business processes and quality of care.

Abbreviations: HRH = human resources for health; M&E= monitoring and evaluation; MSD = Medical Stores Department; NIDA = National Identification Authority; RITA = Registration Insolvency and Trusteeship Agency; SDP = service delivery point.

6 Application architecture

6.1 Introduction

An application architecture defines and categorizes applications used in the health sector, and it provides standards and guidance in areas such as data exchange. The baseline application architecture describes the current setup, and the target architecture defines the major types of applications needed to process data and support operations and which institutions in the health sector should use them and how.

An application architecture has the following objectives:

1. ***Link business strategies and technology.***
   Act as a bridge between the business architecture and the technology architecture by translating business requirements into applications and components to be implemented by the technology architecture.

2. ***Outline application requirements.***
   Map common business requirements in the health-sector building blocks against appropriate applications and components.

3. ***Guide the design and development of digital health solutions.***
   Provide and suggest appropriate application design architectures and software development methods.

4. ***Implement data exchange standards.***
   Provide guidance on how digital health solutions should exchange information in the health-sector ecosystem.

6.2 Architecture principles

Application architecture principles should govern how the application architecture is established and how decisions about applications are made. They can guide decision-makers to decisions that align with health-sector goals. Table 22 describes the guiding principles for application architecture.

Table 22. Application architecture principles.

Principle	Design of user-centered applications
Reference code	TZHEA-AP01
Statement	Digital health solutions should be rooted in an understanding of user characteristics, needs, and challenges. User-centered design—also referred to as *design thinking* or *human-centered design*—starts with getting to know the people you are designing for through conversation, observation, and co-creation. Applications should be designed for or adapted to specific groups of users and should result in good user experiences, efficiency, and expected results.
Rationale	+ To involve and engage users, who should define their system requirements based on the established business processes, rules, and guidelines. + To design tools that improve current user processes, saving them time and using fewer resources; account for users' level of knowledge; and improve quality. + To be open about setting expectations and let people opt out of participating in the design process. + To ensure the usability of applications based on user needs, experience, and challenges as observed and considered from the analysis stage through implementation.
Implications	+ Include user involvement and engagement from the inception of any project that is expected to introduce new applications or information systems. + Consider the level of supporting infrastructure, knowledge level of the users, user support, and maintainability of the systems when designing digital health solutions.

	+ Increase the requirements for standardization of infrastructure and equipment, in accordance with health, safety, and environmental requirements for users and patients. + Develop the tool in an incremental and iterative manner, with a clear purpose and objectives in mind.
Principle	**Understanding of the existing health ecosystem**
Reference code	TZHEA-AP02
Statement	Digital tools should account for the health-sector structure outlined in the business architecture.
Rationale	+ To ensure that selected technology tools will be relevant and sustainable and will not duplicate existing efforts. + To minimize the time needed to implement applications and to maximize impact in the health sector. + To foster collaboration and alignment with existing initiatives. + To ensure the sustainability of digital solutions.
Implications	+ Engage with target users and consult the digital health governance structure to understand existing tools or systems within the health ecosystem (in similar fields, environments, infrastructures, or networks) or with similar worker skill sets before designing an initiative or tool. + Coordinate with the government, implementing organizations, and civil society organizations early on to learn from successful and unsuccessful initiatives in the health ecosystem, avoid duplicating efforts, and more easily integrate with existing technical systems. + Ensure that digital health initiatives align with existing technological, legal, and regulatory policies, and consider policies that are currently in development. + Involve community members, donors, local and national governments, and other implementing organizations throughout the project life cycle. + Monitor the health ecosystem for changes throughout the project life cycle, and adapt products, tools, or initiatives as needed.
Principle	**Data-driven systems**
Reference code	TZHEA-AP03

Statement	When a system is data driven, high-quality information should be available to the right people when they need it, and they should use the data to take action. The data produced by a digital health solution should be used for more than just outputs, such as published work or reporting.
Rationale	To make the correct information available at the right time and place so users can make the right decisions.
Implications	+ Manage information according to internal and external requirements. + Provide decision support through correct information at the right time and place, which is critical to making the right decision. + Measure programs continuously and incrementally, focusing on outcomes, not just outputs. + Make use of existing data, including open datasets and data from interoperable systems. + Use rigorous data collection methods; consider and address potential biases and gaps in the data collected; perform data quality checks; and maintain strong documentation behind the collected data. + Use high-quality real-time or timely data to support rapid decision-making, improve programs, and inform strategy. + Present data in formats that are easy to interpret and act on, such as data visualizations.
Principle	**Privacy and security**
Reference code	TZHEA-AP04
Statement	Privacy and security in the development of digital health solutions involve careful consideration of which data are collected and how they are acquired, used, stored, and shared. Information sharing and disclosure of data, such as patient data, should be done in accordance with relevant legislation and internal policies.
Rationale	To protect information from unauthorized access, use, or disclosure.
Implications	+ Keep the best interests of users and individuals whose data are collected at the forefront of the planning process to uphold

	user privacy and ensure data security and ethical implementation. + Ensure that every person with access to patient-level data and information (both electronic and nonelectronic) adheres to the code of conduct for information security to prevent unauthenticated and unauthorized access to sensitive information. + Minimize the collection of personally identifiable information; consider how critical personal information is to the project's success and what the consequences would be if those data were exposed to third parties. + Assess the risks of unauthorized access or leakage of data; consider the impact of malicious access or publishing of data and the risks of data being combined with other datasets. + To provide access to open information while maintaining data security, identity, and security needs at the data level, not the application level. + Include security in the design of data elements from the beginning; it cannot be added later. + Protect the system, data, and technologies from unauthorized access and manipulation.
Principle	**Interoperability**
Reference code	TZHEA-AP05
Statement	Digital health solutions should be designed so they allow information exchange using defined data standards and information exchange standards and guidelines.
Rationale	To ensure that policies reinforce, and standards define and facilitate, interoperability.
Implications	+ Eliminate a patchwork of information and communication technology solutions that are unable to "talk" to one another or exchange data. + Enable effective interconnection, collaboration, access, and data integration to allow communication between different stakeholders.
Principle	**Sharing, reuse, and collaboration**

Reference code	TZHEA-P06
Statement	Applications should promote reusability of data, build on existing platforms, and facilitate collaboration among organizations during implementation.
Rationale	+ To promote sharing, reuse, and collaboration. + To avoid duplication and loss of time and financial resources. + To shorten the delivery time of digital solutions and thereby improve health outcomes.
Implications	+ Identify common components (including relevant government policies, standards, and existing applications and technology) across the interoperability domain, and define policies, standards, and procedures to ensure the reusability of architecture artifacts (e.g., by defining the data structure and datasets at the government level). + Identify and choose technology tools, standards, and platforms that will enable flexibility and reduce the administrative burden. + Develop modular, interoperable approaches, instead of stand-alone ones, to ensure the ability to adopt and build on components from other software developers or existing applications and the ability of other institutions to perform reciprocal processes in the future. + Collaborate with other digital development practitioners through technical working groups, communities of practice, and other knowledge-sharing events to become aware of existing tools and to build relationships that could lead to the future reuse and improvement of the tools in use.
Principle	**Use of open standards**
Reference code	TZHEA-P07
Statement	Whenever possible, digital health solutions should use or adopt open standards, open source tools, and open innovations and generate open data.
Rationale	+ To use open standards to reduce technology lock-in and promote sustainability of solutions.

	+ To promote competitiveness and opportunity to look at integrated platforms.
Implications	+ Adopt and expand on existing open standards: specifications that have been developed, agreed upon, adopted, and maintained by a global community to enable the sharing of data across tools and systems. + Develop modular, interoperable approaches instead of standalone ones, to ensure the ability to adopt and build on components from other software developers or existing applications and the ability of other institutions to perform reciprocal processes in the future. + Share non-sensitive data after ensuring that data privacy needs are addressed; encourage open innovation by any group or sector, and do not place restrictions on data use. + Use existing open platforms where possible to help automate data sharing; connect tools or systems with other tools and systems and add flexibility to adapt to future needs. + Customize or develop software code to be open source, which anyone can view, copy, modify, and share, and distribute the code in public repositories.
Principle	**Designing for scale**
Reference code	TZHEA-P08
Statement	Digital health solutions should be implemented only if they have a clear plan to scale.
Rationale	To ensure that standards meet the changing and growing needs of public institutions.
Implications	+ Plan and design for scale from the start. + Develop a definition of scale for the digital solution. + Keep the design simple, flexible, and modular to make it easy to change content and adapt to other contexts. + In making technology choices, think about whether they will make it easier or harder to scale. + Identify partners early on who can help scale the tool, system, or approach. + Gather evidence and demonstrate impact before attempting to scale.

	+ Do not attempt to scale without fully validating that the initiative is appropriate in a new context and addresses a high-priority need.
Principle	**Extensibility**
Reference code	TZHEA-P09
Statement	Digital health solutions should be made extensible to accommodate changes to requirements over time.
Rationale	To ensure that digital health solutions are relevant over time and can continue to provide needed services.
Implications	Adapt and respond to changes in requirements and fluctuations in demand in order to adapt to new challenges facing the health sector.
Principle	**Sustainability**
Reference code	TZHEA-P10
Statement	Digital systems and tools should be built and implemented so they are sustainable, can maintain user and stakeholder support, and can maximize long-term impact.
Rationale	To ensure that user and stakeholder contributions are not affected due to interruptions such as loss of funding.
Implications	+ Plan for sustainability from the start. + Develop a definition of sustainability for the initiative or system. + Identify and implement a sustainable business model. + Use and invest in local information technology service providers. + Engage the government and integrate national strategies into programming. + Collaborate instead of competing in order to identify the approach with the greatest impact. + Build a program that can be adapted to user needs.

6.3 Baseline application architecture

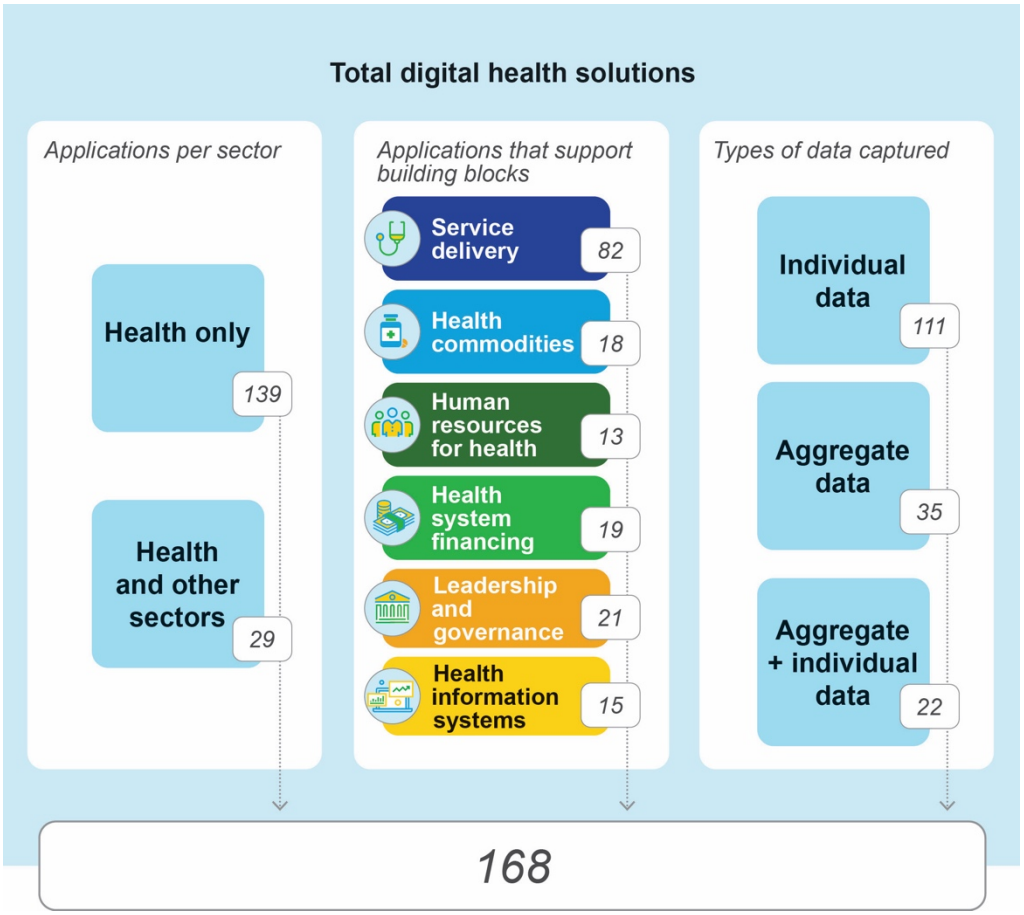
The baseline application architecture describes the current state of applications in the health sector and analyzes how they are designed and managed and how they function and exchange information.

6.3.1 Health-sector applications

More than 160 systems are currently in use in the Tanzanian health-sector ecosystem. Most have duplicating functionalities, not interoperable ones, and do not exchange data.

Figure 18 shows digital health solutions in the health sector distributed based on the building blocks and types of data captured.

Figure 18. Main national-level applications in use in the health-sector ecosystem.



6.3.2 Standards and guidelines

The e-GA has established standards for public institutions to guide the architecture, governance, security, and interoperability of digital health solutions, but no similar standards exist for the health sector. This causes difficulties in the management, interoperability, exchange, and security of information.

A guideline exists that addresses deployment and monitoring of digital health solutions at the facility level: *Guideline and Standards for Integrated Health Facility Electronic Management Systems*. It offers basic standards and guidance for deploying and monitoring digital health solutions at the facility level; it also provides standards for information exchange. However, it does not provide guiding principles for the design and development of digital health solutions.

6.3.3 Application governance

Governance is lacking at different levels of the health-sector ecosystem to guide the design, acquisition, deployment, and operations of digital solutions. This has resulted in the deployment of digital solutions that do not address business needs, technology that is locked in, vendor-dependent solutions, and inadequate sustainability plans.

6.3.4 Digital health solution challenges

The main challenges in implementing digital health solutions are as follows:

1. ***Existence of multiple systems***
   Systems with similar functionality are used at the same SDPs, which creates duplicative functionalities and may result in data inconsistency.

2. ***Lack of a change-management plan***
   Most digital health solutions are implemented without a change-management plan; this results in resistance to using and migrating to the new system.

3. ***Low user skill level***
   Most health applications are deployed without a comprehensive capacity-building plan, which includes training of users on the new system.

4. ***Lack of system documentation***
   Most systems are developed and deployed without proper technical and user-support documentation. This creates difficulty in managing health applications.

6.4 Target application architecture

The target application architecture describes application designs and interoperability standards that can support achievement of the health sector's vision, mission, and objectives.

6.4.1 Standards and guidelines

Health applications should be designed and developed to ensure interoperability in the health ecosystem, as well as enable seamless migration and the addition of new applications or modules to the system without service interruption.

Table 23 describes the recommended standards for developing digital health solutions.

Table 23. Recommended standards for developing digital health solutions.

#	Standard	Description	Recommendations
1	e-GA interoperability standard and guidelines	These standards describe how public institutions' applications should be developed to allow for interoperability.	Digital solutions should adhere to e-GA standards and guidelines for interoperability.
2	Health Level Seven International (HL7®)*	This standard governs the transmission of patient-level data between health systems.	Health systems should be able to exchange defined minimum patient-level data using HL7.
3	Fast Healthcare Interoperability Resources (FHIR®)*	This standard describes data formats and elements and an application programming interface for exchanging electronic health records.	Health systems should use the FHIR standard to exchange health care data and population data.
4	Digital Imaging and Communications in Medicine (DICOM®)**	This is the international standard for transmission, storage, retrieval, printing, processing, and displaying of medical imaging information.	Health systems should exchange medical images and facilitate the development and expansion of picture archiving and

		DICOM enables the transfer of medical images across systems and facilitates the development and expansion of picture-archiving and communication systems.	communication across systems by using DICOM.
5	**International Organization for Standardization (ISO)/Institute of Electrical and Electronics Engineers (IEEE) 11073**	This standard for medical device communications is the base standard of the ISO/IEEE 11073-20000 medical device application profiles.	Health systems should enable communication between medical, health care, and wellness devices. The standard provides an automatic and detailed electronic data capture of client-related and vital signs information and of device operational data.
6	**Global Standards One (GS1®)*** **	GS1 is a common foundation for uniquely identifying, accurately capturing, and automatically sharing vital information about products, locations, assets, and more.	Logistics systems should use GS1 to identify health commodities.

Abbreviations: DICOM = Digital Imaging and Communications in Medicine; e-GA = e-Government Authority; FHIR = Fast HealthcCare Interoperability Resources; GS1 = Global Standards One; HL7 = Health Level Seven International; IEEE = Institute of Electrical and Electronics Engineers; ISO = International Organization for Standardization.

** HL7 and FHIR are registered trademarks of Health Level Seven International.*

*** DICOM® is the registered trademark of the National Electrical Manufacturers Association.*

**** GS1 is a registered trademark of GS1 AISBL.*

In addition to the standards above, Table 24 describes the recommended guidelines for developing digital health solutions.

Table 24. Recommended guidelines for developing digital health solutions.

#	Area	Descriptions	Recommendations

1	**Application programming interface**	Digital health solutions should be built with APIs that enable quick and transparent integration with other health-sector applications and e-government applications, facilitating access to data and services to promote information sharing in the health ecosystem.	For guidance on inclusion of APIs, use *e-Government Integration Architecture – Standards and Technical Guidelines* (eGA/EXT/APA/001).[viii]
2	**Service-oriented architecture**	Digital health solutions should adapt the service-oriented architecture, which facilitates the development of reusable, loosely coupled, flexible, extensible, and vendor-neutral solutions to improve business agility and effectiveness.	Use the service-oriented architecture style, as indicated in *e-Government Application Architecture – Standards and Technical Guidelines* (eGA/Eext/APA/001).[xiii]
3	**Microservices**	For large and distributed digital health solutions, designs can use an advanced service-oriented architecture design style known as *microservice architecture*, which supports distributed development of cloud applications.	Use microservice architecture to address dynamism, scale, and complexity of digital health solutions.
4	**Secure coding practices**	Digital health solutions must adhere to standard secure coding practices (e.g., when designing and implementing access management, session management, password protection, data protection, error handling, and log management).	Standards for secure coding are available in ISO/IEC TS 17961:2013 (Information technology – Programming languages, their environments and system software interfaces — C secure coding rules).

5	**Business intelligence (artificial intelligence and automation)**	To improve health outcomes, digital health solutions can be designed and developed by applying complex algorithms and software to emulate human cognition in the analysis of complicated health data.	Digital health solutions can include business intelligence to support data use for action.

Abbreviation: API = application programming interface; IEC = International Electrotechnical Commission.

6.4.2 Recommended nonfunctional requirements

Table 25 lists recommended nonfunctional requirements that ensure consistent exchange of information and interoperability. The target health application architecture supports the use of technology that is appropriate for the use case and does not preclude the use of proprietary tools but rather supports the use of tools that are built to meet the identified needs and support implementation. It takes an open architecture approach and requires that technologies not create a "lock-in" scenario whereby implementers have no access to their data.

Table 25. Recommended nonfunctional requirements.

#	Area	Recommendation
NFR-1	**Data access and storage**	Technologies should provide standard means of accessing data within the system that do not lock the client into proprietary data formats or storage mechanisms.
NFR-2	**Technical documentation**	The system should be well documented; a digital health solution system should include appropriate background, design, installation, configuration, and operational documentation to ensure that it is easy to understand, maintain, and debug: + Source code should have comments so developers will not need to look elsewhere to understand it. + Configuration files should have embedded comments explaining the different options. + Installation, configuration, and operational activities should be described.

NFR-3	**Integrated development environment and source control**	+ Digital health solutions should be developed in an integrated development environment in order to manage source code complexities, code completion, and dependence management. + If the system is an open source tool, it should provide easy access to source code; a standard version control system (e.g., GitHub) should be used to ensure that source code access is fast and that the code is easy to download, compile, and execute.
NFR-4	**Development technology**	The system should be built using common technology: + To enable easy running, configuration, and debugging, the software should be built on popular technologies that are widely accepted by developers (and use a programming language such as PHP, Java, Python, or JavaScript and a database program such as MySQL, MariaDB, or PostgreSQL). + Any third-party libraries used by the software should be easy for a typical developer to use. + Any external software or systems (such as the database) should be easy to use. + The contents of the database should be easy to view.
NFR-5	**Unit testing**	The source code should include unit tests that are based on the specific requirements of Open Health Information Exchange, that create a framework to validate the functionality, and that the system can operate.
NFR-6	**Open licensing**	An application architecture does not preclude the use of proprietary solutions. If an open source solution is selected, the component should ideally be distributed under an OSI-approved open source license that minimizes complexity and enables an implementer community to reuse and extend functionalities to meet users' objectives.
NFR-7	**Operating environment**	The system should consider the IT infrastructure of low-resource settings where electricity, Internet, and/or technical literacy may be limited.

Abbreviation: IT = information technology; NFR = Non-Functional Requirement; OSI = Open Source Initiative.

6.4.3 Shared services

Table 26 describes recommended shared services for each building block to enable the health sector to achieve the capabilities described in the target business architecture.

Table 26. Recommended shared services for each building block.

#	Building block	Shared service	Description
1	Service delivery	Client registry	Provides a reference repository of identification data on individuals who are accessing health services. This health client registry closely references and links to other broader-than-health shared services, such as civil registration and vital statistics and National Identification Authority services.
2	Service delivery	Shared health records	Contains client health and medical records shared across points of service, including facilitating referrals and continuity of care.
3	Service delivery	Terminology services	Facilitates maintenance and sharing of terminology standards and coding systems and provides a reference data repository with data, metadata, and coding descriptions of clinical observations, diseases, diagnoses, investigations, and other clinical data points according to standards outlined in the data architecture. Such a unified repository is essential to ensure smooth data exchange between different stakeholders or systems.
4	Service delivery	Health facility registry	Facilitates unique identification of health facilities or service delivery points, including name, location, type, status, and services provided.
5	Health commodities	Product registry	Provides lists, regulatory status, and codes for medical supplies and equipment.

6	**Human resources for health**	Health worker registry	Provides a central system to identify and track registration status and employment location of health workers across the public and private sectors.
7	**Leadership and governance**	Administrative areas registry	Provides information about administrative areas, which facilitates the provision of health care services.
8	**Health information systems**	Interoperability layer	Facilitates the exchange of information between applications and various health registries in the health-sector ecosystem.

6.4.4 Digital health solutions

Table 27 describes other recommended digital solutions that should link with shared services to support the health sector in meeting its business needs.

Table 27. Other recommended digital solutions to link with shared services for each building block.

#	Digital health solution	Description
Service delivery		
1	**Health facility digital system**	Facilitates service provision at facilities at all levels. Solutions include those for tracking: + Medical records. + Laboratory and diagnostics. + Pharmacy and stock management. + Facility equipment management. + Revenue. + Facility planning, budget, and expenditure. + Facility-based HR management, including monitoring of attendance.
2	**Diagnostic sample referral system**	Facilitates diagnostic sample referrals and tracks transport of samples between facilities. The solution should be linked with facility systems (medical records and laboratory).

3	**Community health volunteer system**	Facilitates client tracking and services provided by community health volunteers.
4	**Client information, education, and communication system**	Provides educational content and client reminders; can be linked with medical records for more customized content.
5	**Emergency transport coordination system**	Facilitates ordering and tracking of emergency transport (ambulances and alternative transport).
Health commodities		
6	**Health facility regulatory database**	Facilitates applications for registration, fee payments, and approval of registration status of private and faith-based health facilities, including laboratories and drug shops.
7	**Health product regulatory database**	Facilitates applications for registration, fee payments, and approval of registration status of regulated health commodities and equipment.
8	**Supply chain management information system**	Tracks orders, deliveries, and supply of health commodities throughout the public-sector supply chain.
9	**Blood products management information system**	Tracks collection, testing, and supply of blood products.
10	**Infrastructure and equipment maintenance tracking system**	Facilitates inventory management and tracking of maintenance status and maintenance requests for infrastructure and equipment.
Human resources for health		
11	**Health worker communications system**	Facilitates peer-to-peer networking, professional updates and announcements, and other communications to and between health workers.
12	**Health worker qualification,**	Tracks all qualification, training, and CPD undertaken by health workers, in order to facilitate better coordination of training and CPD.

	training, and CPD tracking system	
13	**eLearning platform**	Provides distance learning to health workers and ensures updated skills in the field.
14	**Health worker regulatory database**	Facilitates applications for registration, registration fee payments, and approval of registration status of health workers by different regulatory councils.
15	**HR management information system**	Manages information related to the employment of workers, including payroll and other HR records.
Health system financing		
16	**Systems for planning, budgeting, revenue collection, accounting**	Facilitate management of finance, including planning, budgeting, collection, and accounting.
17	**Health insurance system**	Facilitates insurance enrollment and claims processing.
Leadership and governance		
18	**Client feedback system**	Facilitates collection and processing of and response to client feedback about quality of health services.
19	**Facility supervision system**	Facilitates facility supervision and assessment and follows up on recommendations.
Health information systems		
20	**National Health Data Warehouse**	Acts as national repository of routine health-sector data and statistics.
21	**Event reporting system**	Reports and communicates about disease outbreaks (integrated disease surveillance and response) and other public health–related events, such as adverse drug reactions and disasters, to facilitate national response.

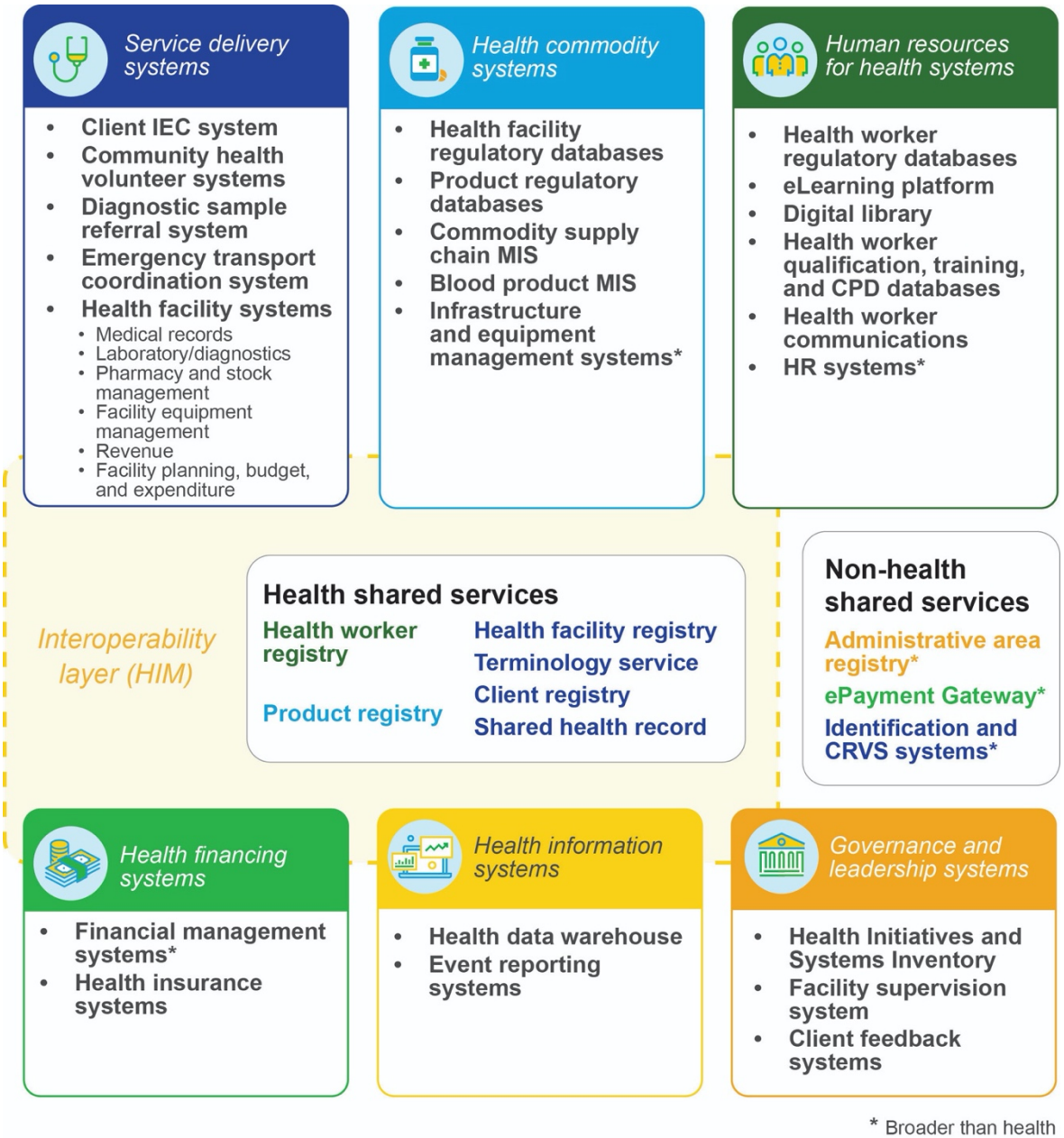
22	**Digital library of health documents**	Acts as a centralized repository of publicly accessible health-sector documents.
23	**Health initiative and systems inventory**	Records all health initiatives and supported digital systems to facilitate coordination.

Abbreviations: CPD = continuing professional development; HR = human resources.

6.4.5 Application architecture overview

Figure 19 shows the various digital health solution categories in the health sector (in the outer part of the figure) and the shared services (in the center). Health sector–specific systems are depicted using a rounded shape, and systems with a scope broader than health have sharp corners. Items are grouped by color according to health-sector building block: service delivery, health commodities, human resources for health, health system financing, leadership and governance, and health information systems.

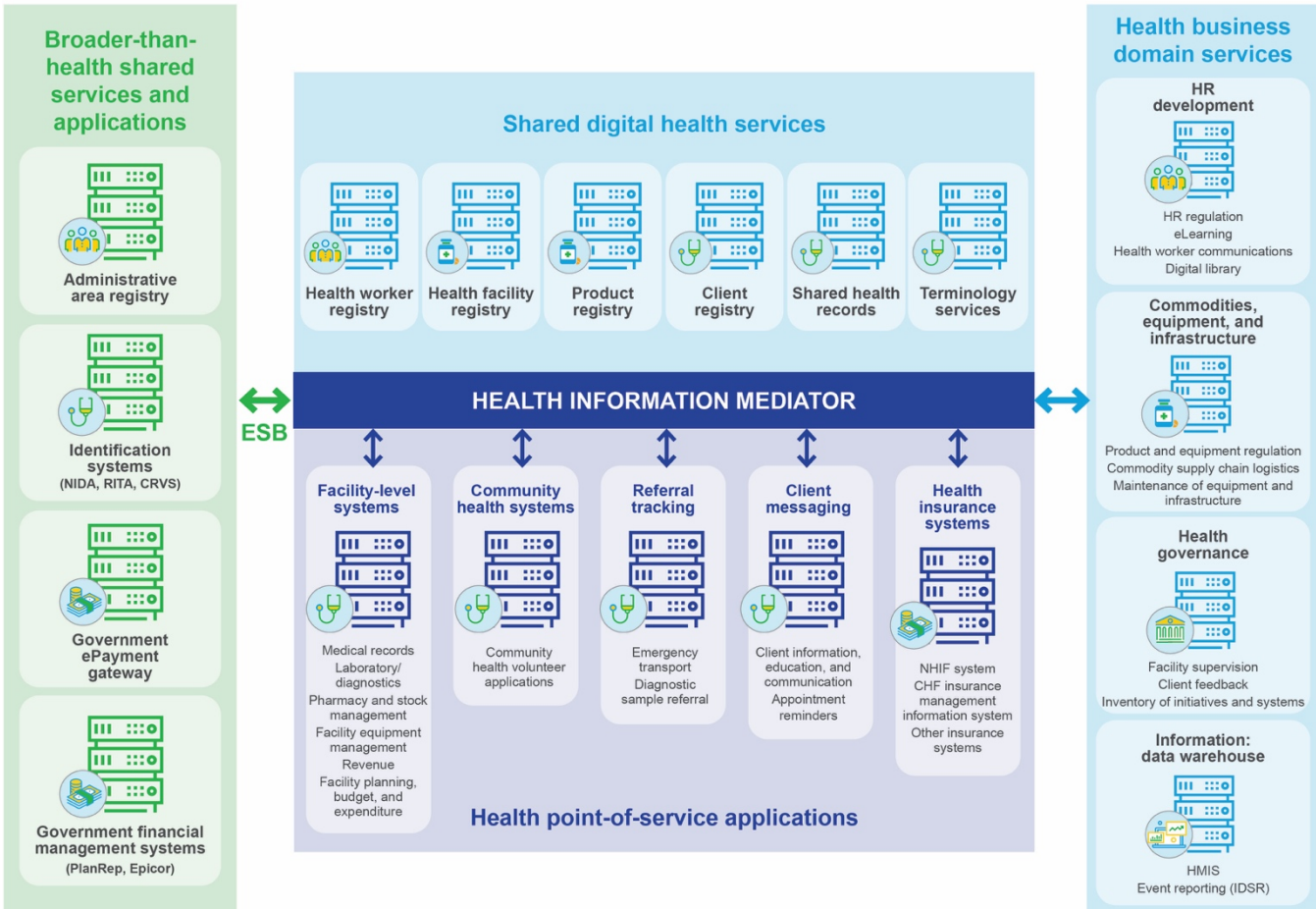
Figure 19. Categories of digital health solutions and shared services.



Abbreviations: CPD = continuing professional development; CRVS = civil registration and vital statistics; HIM = health information mediator; HR = human resources; IEC = information, education, and communication; MIS = management information system.

Figure 20 shows the core applications for each building block.

Figure 20. Application architecture layers.



Abbreviations: CHF = community health fund; CRVS = civil registration and vital statistics; ESB = enterprise service bus; HMIS = Health Management Information System; HR = human resources; IDSR = integrated disease surveillance and response; NHIF = National Health Insurance Fund; NIDA = National Identification Authority; RITA = Registration Insolvency and Trusteeship Agency.

6.5 Gap analysis and recommendations

Table 28 describes gaps in the baseline application architecture and corresponding recommendations.

Table 28. Gaps in the baseline application architecture and corresponding recommendations.

#	Baseline gap	Recommendation
1	**Reference registries**	Different systems should use reference registries for common data, such as locations and health worker records.
2	**Standard application programming interfaces**	Different applications should use a guideline with standard API formats to allow for interoperability.
3	**Standard functional requirements**	All systems should meet a generic set of minimum functional requirements.
4	**Standard nonfunctional requirements**	All systems should meet a generic set of minimum nonfunctional requirements.

Abbreviation: API = application programming interface.

7 Technology architecture

7.1 Introduction

A technology architecture focuses the physical environment and aspects of the health sector's IS, including the computer network infrastructure, data administration, and recommended standards and guidelines.

7.2 Architecture principles

Table 29 describes the TZHEA technology architecture principles.

Table 29. Principles guiding the Tanzania Health Enterprise Architecture technology architecture implementation.

Principle	Interoperability
Reference code	TZHEA-T01
Statement	Software and hardware should follow established standards that promote the interoperability of data, applications, and other technology.
Rationale	+ To help ensure coherence, improve the ability to manage systems, increase user satisfaction, and protect current information technology investments, thus maximizing return on investment and reducing costs. + To help ensure support from several suppliers for their respective products, which can facilitate integration.
Implications	+ Ensure that interoperability standards and industry standards are followed unless a compelling business reason exists to implement a nonstandard solution.

	+ Establish a process for setting, reviewing, and revising standards periodically, as well as for granting exceptions. + Identify and document existing information technology platforms.
Principle	**Infrastructure resilience and scalability**
Reference code	TZHEA-T02
Statement	Software and hardware should be built and set up to support business continuity, ensuring that operations can be resumed at the last recorded state despite potential technical and nontechnical failures.
Rationale	+ To provide resilience, which entails availability, archival, and backup. + To support overall service-level agreements for maintaining information and communication technology infrastructure and addressing availability and performance issues.
Implications	+ For scalability, ensure that the chosen technology standards meet evolving health-sector needs and requirements and that the applications and technologies can scale up to adapt to such changes and demand fluctuations; and ensure that server, storage, and network capacities can handle user, application, and data loads. + For availability, ensure that the technology infrastructure has no single point of failure. + For archiving and backup, ensure that the infrastructure has data and data sources spanning multiple years; and ensure that the archiving and backup policy and mechanism address the archival and backup requirements of the system and are aligned with the health sector's ethical and regulatory requirements. + Consider failover requirements when designing the system infrastructure, and ensure that a single server or network link failure does not bring down the entire system (even though, for example, performance may degrade). + Ensure that the system handles every request and yields responses, errors, and exception conditions effectively. + Ensure that, in the event of a failure or crash, recovery of transactions and data is possible.

	+ Ensure that the platform solution will support effective disaster recovery.

7.3 Standards and guidelines

This section describes recommended technology standards and guidelines.

7.3.1 Network

1. For all sites, platforms, and systems operating online and/or in a network, the network infrastructure should have high-quality, reliable, scalable, and measurable connectivity that is always available. Mission-critical sites must be engineered for fault tolerance. This implies that, in mission-critical sites such as server rooms or computer rooms, networks should be configured to ensure no single point of failure.
2. All sites, platforms, and systems should maintain accurate and up-to-date network topology diagrams and documentation. The documentation is required primarily for network issue isolation and troubleshooting. In addition, preparations for growth, infrastructure upgrades, or architectural redesign require a comprehensive understanding of the current network topology.
3. All sites, platforms, and systems should use sound design principles, open standards, and long-range planning for core network services such as Directory Services, Domain Name System (DNS), and Internet Protocol (IP) addressing (using Dynamic Host Configuration Protocol) in a structured manner. These require careful consideration not only during network design but also during physical implementation.
4. Network setup should factor in tools, features, and services that will enforce and protect clients' data security and privacy, facilitate access on the network, and provide audit logs for reconstructing or data-breach events, etc.
5. All workstations on the network should have the fundamental tools for self-protection, including a personal firewall, spyware/malware protection, disk-based data encryption, and basic security reporting.
6. All network deployment should facilitate each of the following key network management functions: network discovery process, network topology visualization, availability management, incident management, ICT asset management, configuration management, performance management, and problem management.

7. Networks should provide application response times that are acceptable to support business needs and have cost-effective bandwidth to satisfy the current and future networking needs of application users.
8. ICT policies should clearly indicate what information should be available and accessible over the extranet, Internet, and intranet. Intranet should always be considered for sharing highly sensitive information, especially client-related information. Whenever applicable, no individual-level client data should be shared using an extranet or the Internet. For such sharing and transfers, the first consideration should be to transfer information in aggregate; if client-level information must be transferred, it should be encrypted and possibly sent over a virtual private network (VPN).
9. All network appliances (Secure Sockets Layer accelerators, Net Cache devices, Extensible Markup Language appliances), devices (routers, switches, VPN devices, hubs, firewalls), and telephony devices (dialers, automatic call distributors, interactive voice responses, private branch exchanges) should be procured and set up according to guidelines developed by the MoHCDGEC's ICT unit.

7.3.2 System software

1. ***Server operating systems***

   All servers should run the most recent version of the server operating system. In addition to providing additional features and functionality, the most recent version will improve the overall security of the server's data and services. The MoHCDGEC's ICT unit will develop guidelines for periodic reviews of operating systems and required guidelines. Server support and maintenance plans should include upgrades.

2. ***Network operating system (NOS)***

   Both the peer-to-peer NOS and the client/server NOS should support, at a minimum, protocol and processor support; hardware detection and multiprocessing; printer and application sharing; common file system and database sharing; network security capabilities such as user authentication and access control; directory, backup, and web services; and internetworking.

3. ***Desktop operating system (DOS)***

   For end users, the most recent version of Microsoft Windows is the recommended DOS. Linux DOS is the recommended DOS for desktops and workstations used by ICT specialists who will potentially have access to alter platforms and application settings. Plans should be made for regular DOS patching and service

pack updating. Regular program cleanup should be conducted to remove unnecessary and potentially damaging programs.

4. ***Domain Name System (DNS)***
   To allow for redundancy, at least two DNS servers should be set up to serve the same purpose and use Active Directory Integrated DNS zones for easy deployment. After DNS servers are set up, special attention should be paid to replication, redundancy, simplicity, and security.

7.3.3 Web infrastructure

1. Whenever applicable, separate servers should be used for internal and external applications. This will limit harm from malicious attempts to access external applications with the aim of intruding into internal applications.
2. Separate application servers should be used for production, testing, and debugging. Whenever possible, a separate training server (a replica of the production server in terms of features) should be used.
3. Web-access activities should be continuously audited, and logs should be stored in a secure location. Whenever possible, logs should be stored in a device that is virtually and physically secure. Digital means such as encryption with digital signatures may be used to prevent scam modifications.
4. The terms and conditions of application vendors and developers should include adherence to sound security coding practices.
5. The system should support work in offline mode for mission-critical systems such as electronic medical records.

7.3.4 Data administration

1. All centralized platforms and systems should allow information and application access from anywhere. This can be done by deploying role-based configurations. Virtual machines can be used for users, independent of hardware and operating systems, to provide seamless migration for mobile computing, enable personalized applications and computing environments anywhere, and provide shared server-based computing for task workers using centrally stored data.
2. Stakeholders should consider the following general requirements for use of mobile data storage:

   2.1 *Correct use of mobile data storage devices*

   + Platform and system users should be educated in the safe use of ICT before they start using the devices.

+ Platform and system users must use the mobile data storage devices only for business/work. Mixing official information and private information on the same device should be prohibited.
+ Data files transported via devices such as flash drives, portable hard drives, mobile phones, and tablets must be deleted from those devices once the transfer process is complete.
+ Platform and system users must not use CD-ROMs, DVDs, or backup tapes for transfer or storage of information for future uses. These are classified as redundant technologies and should not be supported.
+ Whenever applicable and possible, stakeholders should adhere to POPSM&GG directives when procuring mobile data storage devices.

2.2 *Registration of mobile data storage devices*

+ Mobile data storage devices should be registered in the institution's ICT asset registry using user information.
+ Transfer of mobile data storage devices must adhere to regulations on the issuing of office equipment.
+ Mobile data storage devices must be stored in the appropriate offices for the safekeeping of information and equipment. Any user who needs to take a storage device out of the designated office must inform the relevant authorized person.
+ Any loss of a mobile data storage device must be reported to the appropriate authority immediately so necessary actions can be taken.

2.3 *Destruction/decommissioning of mobile data storage devices*

+ When a mobile data storage device is no longer needed (when it becomes obsolete), it must be destroyed according to the institution's policies. When applicable, such devices must be sent to the Directorate of Records and Archives Management for destruction.
+ Selling, giving as a gift, or switching the ownership of a mobile data storage device containing health records before appropriate data destruction measures are taken is prohibited.

3. Whenever possible, health-related data and systems should use the GoT's data centers. When data are stored at GoT data centers, data storage should adhere to the e-GA's guidelines on data storage. At a minimum, all data centers should include a clear policy and documentation on power grid architecture, power distribution units, and a power backup plan (including automatic generators and

fuel capacity and distribution management). The policies and documentation should also cover wiring management, rack management, and physical security.

4. Public institutions must comply with the *Government Data Centers Guidelines and Procedures* (eGA/EXT/IRA/002) when using data center services provided by the e-GA.

7.3.5 Monitoring and control management

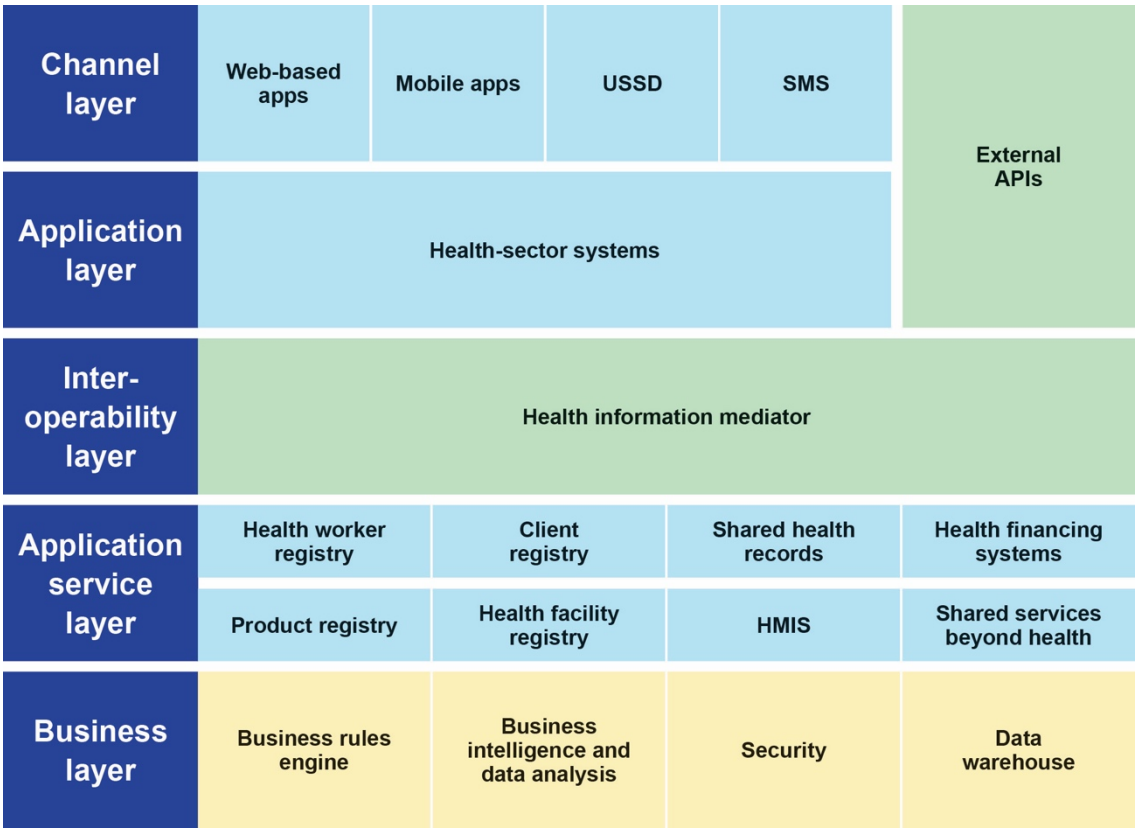
1. Stakeholders in the health sector should use the Information Technology Infrastructure Library, a set of concepts and policies for managing ICT infrastructure, technology, development, and operations. The library describes in detail a number of important ICT practices and includes comprehensive checklists, tasks, and procedures that stakeholders can tailor to their needs.
2. Stakeholders in the health sector should develop ICT acquisition, development, and maintenance procedures with guidance from the e-GA's *Creation of ICT Acquisition, Development and Maintenance Procedure – Technical Guide* (eGA/EXT/IRA/003). To ensure sustainability, costing and budgeting should be key aspects of support and maintenance plans and procedures development.
3. Stakeholders in the health sector should develop institutional ICT service management procedures with guidance from the e-GA's *Creation of ICT Service Management Procedures – Technical Guide* (eGA/EXT/IRA/002). They should consider developing ICT service support and delivery within the organization to ensure that the end user can make optimal use of the technological platform. Services to consider include:
    a. ***ICT asset management***—to have an inventory of all ICT assets and to manage their life cycle.
    b. ***Incident management***—to restore normal service as quickly as possible and minimize the adverse impact on business operations.
    c. ***Service request management***—to enable ICT users to request and receive standard services within a predefined time frame.
    d. ***Help desk management***—to provide a standardized framework for registering and resolving reported ICT issues.
    e. ***Change management***—to ensure that standardized methods are used for the efficient and prompt handling of all changes, that changes are recorded in a configuration management system, and that overall business risk is minimized.
    f. ***Problem management***—to prevent problems and resulting incidents, eliminate recurring incidents, and minimize the impact of incidents that cannot be prevented.

g. ***Capacity management***—to provide a point of focus and management for all capacity- and performance-related issues (relating to both services and resources) and to match ICT capacity to the agreed business demands.
h. ***Configuration management***—to ensure that all hardware and software are configured according to leading practices and appropriately hardened.
i. ***Availability management***—to ensure that ICT systems meet the availability requirements of the health sector through adoption of appropriate disaster recovery mechanisms.
j. ***Release management***—to ensure that stakeholders include the appropriate checks and controls before deploying new hardware and software within the production environment.
k. ***IT service continuity management***—to put appropriate redundancies and mechanisms in place to minimize downtime and ensure uninterrupted service delivery to all users and key stakeholders.
l. ***Service catalog and service management***—to assist the ICT team in selecting ICT services based on business needs and the technical capabilities of the ICT team.

4. Health-sector stakeholders should make use of all e-GA initiatives, including the Government Network, Government Mailing Systems, Government Data Centre, and Government Mobile Platforms.
5. All platform, application, and device management policies should clearly highlight a compliance management plan to address data loss prevention and login monitoring.

Figure 21 depicts the recommended technology architecture framework, which includes standards and guidelines for servers, workstations, storage and network infrastructure, software licensing, ICT vendor management, HR, and service support. It shows a typical infrastructure architecture for a public institution that takes into consideration different layers.

Figure 21. The recommended technology architecture framework.



Abbreviations: API = application programming interface; HMIS = health management information system; SMS = Short Message Service; USSD = Unstructured Supplementary Data Service.

7.3.6 External access, exchange, and delivery of service components

Table 30 provides the reference framework for standards and specifications to support external access, exchange, and delivery of service components or capabilities.

Table 30. Reference framework for external access, exchange, and delivery of service components.

Service type	Service component	Service component guide
Access channels—the interface between an application and its users (e.g., a browser,	+ Web browser + Web access standards (WCAG) + Mobile devices + Collaboration and communications	+ Recommended web browsers: Microsoft Internet Explorer, Mozilla Firefox, Opera, Safari, Google Chrome + Recommended web access standards: WCAG (W3C web

smartphone, or tablet)		accessibility guidelines), ISO 9241-151:2008 (Guidance on World Wide Web user interfaces) + Recommended mobile device categories: feature phones, smartphones, tablets + Recommended collaboration and communications channels: SMS, interactive voice response, Voice over IP, email, social networks
Delivery channels	+ Internet + Intranet + VPN	+ Whenever applicable, all communications should be via a VPN. + The recommended Internet standards are as defined by the Internet Engineering Task Force.
Interconnection	+ Enterprise-level IP network + Application-layer protocols + Transport-layer protocols + Internet-layer protocols	+ Recommended enterprise-level IP network: IPv6 + Recommended application-layer protocols: DNS, DHCP, FTP/FTPS, HTTP/HTTPS, IMAP, IRC, LDAP, MIME, SNMP, POP3, RIP, SMTP, SOAP, SSH, Telnet, etc. + Recommended transport layer protocols: TCP, UDP, DCCP, ECN

Abbreviation: WCAG= Web Content Accessibility Guidelines.

7.3.7 Interfacing with service components

Table 31 provides guidelines for interfacing with service components.

Table 31. Recommended tools and technologies for interfacing with service components.

Service type	Service component	Recommendations
Process integration	+ Business process mapping + Workflow engine + Rule engine	Recommended tools: + Business Process Model and Notation + Business Process Execution Language

		+ Business Activity Monitoring
Application/ service integration	+ Enterprise application integration middleware + Enterprise service bus + Object request brokers + Remote procedure calls + Service discovery and description	Recommended tools and technologies: + Message-oriented middleware (IBMMQ, MSMQ, JMS, JMX) + Object request brokers: CORBA, COM, DCOM + Service discovery: UDDI + Service description: WDSL, API
Data integration	+ Data exchange and transformation + Data exchange format and classification + Data integration meta language + Interoperable character set + Extract, transform, and load	Recommended tools and technologies: + Character encoding for information interchange: ASCII, Unicode, UTF-8 + Data description: XML (first preference), JSON, RDFXNAL, XCIL, XCRL + Data exchange and transformation: XMI, XSLT, ISO 8601 for data element and interchange format + Data exchange formats: UN/EDIFACT, EDI, XML/EDI, XLINK, PDF, .doc, .ppt, .xls, TIFF, JPEG, RTF, MPEG, PST, CSV, HTM, AVI/MP3/MP4 + Ontology-based information exchange: OWL + Data integration meta language: XML + Signature and encryption: XML (first preference), DSS + Key management specifications: SAML, XACML + Data types / validation: XML Schema (first preference), DTD + Data transformation: XLST
Payment mechanism	Service interface with payment mechanisms	Recommended channel: Government Electronic Payment Gateway

external Integration		

7.3.8 Distributed or service-oriented architectures for service components

Table 32 recommends tools and technologies for building, exchanging, and deploying service components across distributed or service-oriented architectures.

Table 32. Recommended tools and technologies for deploying service components across service-oriented architectures.

Service type	Service component	Recommendations
Presentation/user interface	+ Static display + Dynamic/server-side display + Content rendering + Wireless/mobile/voice	Recommended tools and technologies: + Static display: HTML, PDF + Dynamic/server-side display: PHP (first preference), JSP, ASP, ASP.NET + Content rendering: examples include DHTML, XHTML, CSS, X3D + Wireless/mobile/voice: WML, XHTMLMP, Voice XML
Business service component	+ Lines of business/application business logic + Web services + Common utilities + Reusable components	Recommended tools and technologies: + Application business logic + Platform independent: EJB, C++, JavaScript + Platform dependent: C#, VBScript

Data management	+ Database connectivity + Data access objects / object-relational mapping (ORM) + Data validation, cleansing/de-duplication + Data backup and archiving	Recommended tools and technologies: + Data exchange: XMI, XQuery, SOAP, ebXML, RDF, WSUI + Database connectivity: DBC, ODBC, ADO, OLE/DB, DAO, DB2 Connector
Business intelligence and reporting	+ Business intelligence tools and standards + Reporting tools and standards + Search technology	Recommended tools and technologies: + OLAP + XBRL + JOI.AP + XML
Security management	+ Access management + Anti-spam/antivirus + Desktop and enterprise firewall + Identity, authentication, authorization, and privacy + Single sign-on / identity management + Email security + Public key technology + Intrusion detection and prevention + Proxy servers / directory services + Remote security + Secured transport + XML security + Electronic fingerprinting	Recommended tools and technologies: + Access management: support for OS, app server, DBMS, IDM and directory service standards, password encryption during storage and transmission + Digital signatures: secure hash algorithms, authentication, message integrity, non-repudiation + Email security: S/MIMEv3 + Encryption algorithm: DES, triple DES + Identity, authentication, authorization, and privacy: SAMLv1.1, X.509 for identity certificates + Identity management: support for OS, app server, DBMS, IDM, and directory service standards, password encryption standards for storage and transmission + IP security: IPSec

		+ Proxy server: compatible with LDAPv3, able to integrate with adopted standards for directory services + Remote security: SSH + Secure transport: TLS/SSL, XML + Security standards: WS-Security, WS-1 Basic Security Profile, XML-DSIG

7.3.9 Delivery and support platforms

Table 33 recommends tools and technologies to support the construction, maintenance, and availability of service components related to delivery and support platforms.

Table 33. Recommended tools and technologies for service components related to delivery and support platforms.

Service type	Service component	Recommendations
Database/ storage	+ Structured data storage + Unstructured data storage + Storage devices	Recommended tools and technologies: + Structured data storage (DBMS): MySQL, DB2, Oracle, SQL Server, Postgres SQL, Sybase + Unstructured data storage: content server, GIS server + Storage devices: NAS, SAN
Platform and delivery servers	+ Web servers + Application servers + Portal servers + Content servers + Media servers + Desktop OS + Mobile OS + Server OS	Recommended tools and technologies: + Wireless/mobile: J2ME + Platform independent: Linux, JEE, Eclipse + Platform dependent: Windows, .NET, Mac OS + Web servers: Apache, IIS + Media servers: Windows Media Services + Application servers: WebLogic, WebSphere, JBoss, ILOG, Oracle Business Rules, JRules + Portal servers: Liferay, JBoss portal, Oracle WebCenter + Content server: Alfresco

		+ DOS: Windows, Mac, Linux + Server OS: Windows Server, Linux + Mobile OS: Android
Hardware/ infrastructure	+ Servers/computers + Embedded technology devices + Peripherals + Wide Area Network (WAN) + Local Area Network (LAN) + Network devices/standards	Recommended tools and technologies: + Servers/computers: enterprise server, mainframe + Embedded technology devices: RAM, RAID, microprocessor + Peripherals: printer, scanner, fax, cameras + WAN: Frame Relay, DSL, Metro Ethernet, ATM + LAN: Ethernet, VLAN
Software engineering	+ Modeling process, application and data design + Integrated development environment + Application development framework + Programming language for application development + Testing tools + Configuration management software + Commercial off-the-shelf (COTS) software	Recommended tools and technologies: + Modeling process, application and data design: Business Process Model and Notation for process modeling, BPEI4WS for web services, ERD for data modeling, UML 2 and above for application modeling, XML Schema v1.0, WML v2.0 + Integrated Development Environment: RAD, Visual Studio, Eclipse, NetBeans, JDeveloper + Application development framework: use of enterprise framework for app development, support for reuse of existing components and services, support for creating web services. + Programming language for application development: Language should allow for code portability, code collaboration, and browser compatibility and should be compatible with the application development framework adopted. + Testing tools: Tools should be selected for functional testing, usability testing, performance, load and stress testing, security testing, reliability testing, and regression testing.

		+ Software configuration management: Tools should be used for version control, defect tracking, issue tracking, change management, release management, requirement management, and traceability. + COTS software: Applications should support open standards and other industry standards that promote interoperability with other products/vendors, support access to training, and allow parameterization and customization for local needs.

8 Information system security

IS security should ensure that data and applications are accessible to authorized individuals and systems for business purposes in a manner that ensures confidentiality, integrity, and availability.

8.1 Security domains and recommendations

The TZHEA has adopted the GoT ICT security domains as outlined in the e-Government Act (2019). The domains should guide all related security concerns in managing IS in the health sector.

Table 34 describes the security domains and corresponding recommendations.

Table 34. Tanzania Health Enterprise Architecture security domains and corresponding recommendations.

#	Domain	Recommendations
1	**IS security governance and management**	+ Different implementation levels should have a clear policy and IS security strategy that governs how the IS should be managed. + Supportive supervision and technical review should include assessment of IS security risks.
2	**IS security operations**	+ IS operations should be monitored to assess adherence to established policies and strategies. + IS networks should be secured and regularly assessed to prevent intrusion and misuse.

		+ IS testing should include security testing and checking for potential security and confidentiality risks.
3	**Security of ICT assets**	+ The assets register at different implementation levels should include documentation of data storage devices and data generated/managed. + Disposal of ICT assets must adhere to established government guidelines and regulations.
4	**Identity and access management**	+ Data should be made accessible to users only on the basis of verified business needs. + Clients should be informed about what parts of their data will be accessible, by whom, and in what business operations. + Access to information resources should be monitored for appropriate usage and be revoked when access is no longer required. + Supportive supervision and technical assessment of the IS should include a review of access to data, use of administrative functions, and suspicious data usage or requests. + Clear guidelines should govern who can request access to which information resources and how. + Clear guidelines should govern who can share and/or communicate data from different implementation levels and how.
5	**IS security incident management**	+ Clear guidelines should govern reporting of data breaches or misuse at all implementation levels.
6	**IS continuity management**	+ Proper data backup and restoration mechanisms for data systems continuity should be in place at all implementation levels. + A data disaster recovery plan should be in place at all implementation levels. + IS technical testing should include disaster recovery testing and backup and restoration mechanisms. + Supportive supervision and technical assessment should include a review of disaster recovery plan implementation.

7	**IS acquisition, development, and maintenance**	+ Business requirements for new systems or upgrades should include data security and confidentiality controls. + Technical testing of systems should include a review of whether the system is designed and developed according to outlined data security and confidentiality controls.
8	**HR security**	+ All HRH staff who will have access to various types of data should be thoroughly examined and approved based on their business needs and ethical clearances. + HRH staff should be granted access only to data that are relevant to their specific duties, responsibilities, and service areas. + HRH capacity should be built for digital and nondigital data security and confidentiality risks, standards, and guidelines.
9	**Physical and environmental security**	+ Physical access to data storage repositories should be protected against unauthorized access, damage, interference, and environmental threats. + Data should be processed and/or hosted only by available government facilities or government-approved suppliers. + All access to data repositories and maintenance activities should be documented and made available to relevant authorities.
10	**IS security compliance and audit**	+ Periodic internal and/or external independent data audits should be conducted at all implementation levels.

Abbreviations: HR = human resources; HRH = human resources for health; ICT = information and communication technology; IS = information system.

8.2 Security service recommendations

The following security services are recommended:

1. ***Identity management services***

An identity management service should be used for provisioning, authenticating, authorizing, managing, and deprovisioning users.

2. ***Network security services***

   Appropriate measures and tools should be used for network security, including a network intrusion detection system that regularly monitors and scans the network, checking for suspicious activities and malicious attempts. Network security services should also include firewall protection.

3. ***Zoning***

   Zoning should be used to limit unnecessary overlaps of applications and access. Zoning may include use of web zones, application zones, database zones, messaging zones, demilitarized zones, and file exchange zones.

4. ***Layered protection***

   Layered security settings should be deployed, combining multiple mitigating security controls to protect assets (e.g., users, data, and devices). The security strategies should be designed to slow, block, delay, or hinder threats until they can be completely neutralized.

5. ***Security infrastructure and authentication standards***

   Refer to *e-Government Security Architecture – Standards and Technical Guidelines* (eGA/EXT/ISA/001).

6. ***Mobile applications***

   Use a mechanism to wipe the data if the device is lost.

9 TZHEA governance

9.1 Introduction

This section provides a governance structure to guide the implementation, harmonization, and management of health applications in the health sector and ensure alignment of business strategies and ICT initiatives within the health sector. The governance structure ensures that all digital health solutions introduced by the government and the private sector adhere to TZHEA standards.

The governance structure and processes for TZHEA are derived from existing health-sector governance structures for health-sector dialogue and coordination. They divide management of the health sector into three levels: from lowest to highest, they are the implementation level, the technical level, and the policy level.

The technical level is responsible for coordinating health-sector strategic priorities, ensuring equity in resource management, strengthening policy alignment, and reducing transaction costs. Activities under the technical level are performed through various TWGs in defined thematic areas. EA functions are linked to the ICT and M&E TWG.

9.2 TZHEA governance structure and processes

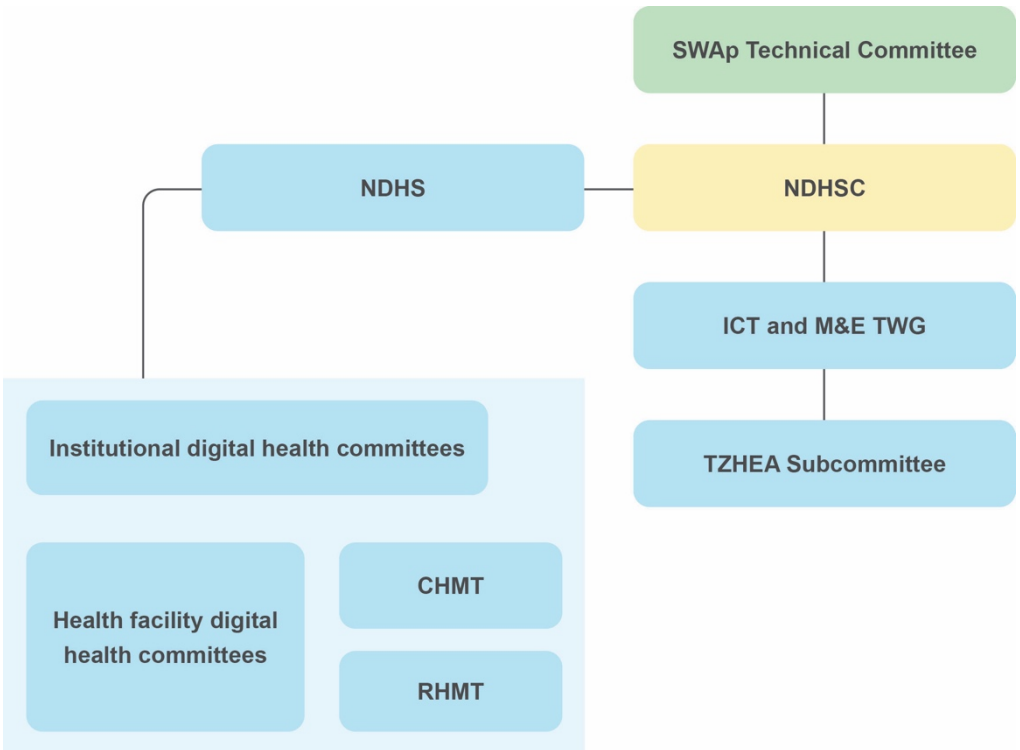
9.2.1 TZHEA governance structure

Digital health solutions are strategically guided by the NDHSC to ensure alignment between health-sector priorities and digital health investments. The ICT and M&E TWG is responsible for managing the implementation of the TZHEA through a subcommittee that leads the implementation of the TZHEA and has dual reporting to the SWAp governance structures and the NDHSC. The senior management of the MoHCDGEC is responsible for ensuring that the TZHEA is implemented.

The TZHEA's governance structure, depicted in Figure 22 and detailed in Table 35, consists of the following:

1. ***SWAp governance structures.***
2. ***NDHSC.***
3. ***ICT and M&E TWG.***
4. ***TZHEA Subcommittee.***

Figure 22. Governance structure of digital health solutions and initiatives in Tanzania.



Abbreviations: CHMT = council health management team; ICT = information and communication technology; NDHS = National Digital Health Secretariat; NDHSC = National Digital Health Steering Committee; RHMT = regional health management team; SWAp = sector-wide approach; TWG = Technical Working Group; TZHEA = Tanzania Health Enterprise Architecture.

Table 35. TZHEA governance team members and their roles.

#	Entity	Members	Roles/Description
Area 1: Overseeing TZHEA implementation			
1	**SWAp**	+ Members of various committees of the health sector SWAp arrangements,	+ Manages development and implementation of the health policy, health

		including technical working groups, TC-SWAP, JAHSR and policy meetings.	strategy, and health-sector strategic priorities. + Centrally coordinated by the Health Sector Reform Secretariat.
2	**NDHSC**	+ PSH, MoHCDGEC + Deputy PSH, PORALG + Chief medical officer + Director of ICT, MoHCDGEC + Director of ICT, PORALG + Director of Policy and Planning + Chief accountant + Director of the Legal Unit + Chair of DPG + CEO of e-GA + Representative from regional medical officers + Representative from district medical officers + Representative from APHFTA + Representative from Christian Social Services Council + Representative from BAKWATA + Representative from academia	+ Co-chaired by the PSH at the MoHCDGEC and the Deputy PSH at PORALG. + Also includes co-opted members from institutions such as relevant Ministries, Departments and Agencies; private-sector, research, and training institutions; and development and implementing partners. + Provides leadership and strategic guidance to the TZHEA. + Mobilizes resources for digital health initiatives and TZHEA implementation activities.
Area 2: Approval and enforcement of the TZHEA blueprint			
3	**ICT and M&E TWG**	+ Director of ICT, MoHCDGEC + Assistant Director of M&E, MoHCDGEC + Director of ICT, PORALG + Program officers + Implementing partners working on digital health + FBOs + Civil society organizations + Private sector	+ Approves, enforces, and promotes the TZHEA and its associated standards, guidelines, and recommendations. + Assigns appropriate resources for implementation of the TZHEA.

			+ Maintains the project development and implementation plans and ensures that TZHEA standards and guidelines are incorporated into the design of the proposed projects and initiatives. + Resolves escalations.
Area 3: TZHEA change agents			
4	**TZHEA Subcommittee**	+ Assistant Director, Public and Private Health Services Section, MoHCDGEC + Assistant Director, Division of Health Services – Health, PORALG + Head of section from the ICT Unit (should not be Director of ICT), MoHCDGEC + Officer – M&E, MoHCDGEC + Officer – Directorate of Curative Services, MoHCDGEC + Officer – Directorate of Preventive Services, MoHCDGEC + Officer – Directorate of Human Resource Development, MoHCDGEC + Officer – DICT, PORALG + Officer – TZEA, e-GA + Officer – ICT, MoWTC + Officer – Health PMO + Officer – MoFP + Officer – Tanzania Communication Regulatory Authority	+ Reviews, monitors, manages, and drives development of the TZHEA according to e-government standards and guidelines as well as the health-sector's vision, goals, and strategies. + Conducts reviews of existing applications/digital health solutions against TZHEA guidelines and standards and advises the NDHSC on appropriate actions. + Ensures compliance of digital health solutions with TZHEA principles, standards, and guidelines in the business, data, application, and technology domains. + Reports to the ICT and M&E TWG, NDHSC, and the Centre for

		+ Advisors: members representing implementing partners	Digital Health on progress made in implementing the TZHEA.
5	**Institutional digital health committees**	Existing members of the ICT Steering Committee within institutions; the TZHEA is part of the committee's permanent agenda, and the committee may form a task team responsible for the TZHEA at the institutional level.	+ Provide technical guidance to stakeholders and technical assistance on architecture segments and the formulation of their respective EA reference models. + Develop, manage, and govern their institution's EA in compliance with the TZHEA and the GoT EA. + Report monthly, quarterly, and annually to the TZHEA Subcommittee through the NDHS on progress and compliance with TZHEA implementation.
6	**Health facility committee**	Existing members of the Health Facility Governing Committee; the TZHEA is part of the permanent agenda of the Facility Governing Committee or the committee responsible for guiding digital health solutions, which may form a task team responsible for the TZHEA at the facility level.	+ Provides technical guidance to stakeholders and technical assistance on architecture segments and the formulation of respective EA reference models. + Develops, manages, and governs health facility EAs in compliance with the TZHEA and the GoT EA.

			+ Reports monthly, quarterly, and annually to the TZHEA Subcommittee through the NDHS on progress and compliance with the TZHEA implementation.
7	**RHMTs**	Existing members of the RHMT in designated councils; the TZHEA is part of the permanent agenda of the regional councils, which may form task teams to work on the health enterprise architecture at the regional level.	+ Advise on changes to the TZHEA based on the architecture standards and changes to the requirements. + Monitor implementation and compliance of digital health investments in accordance with the TZHEA at the regional level. + Report monthly, quarterly, and annually to the TZHEA Subcommittee through the NDHS on progress and compliance with the TZHEA implementation.
8	**CHMTs**	Existing members of the CHMT in designated councils; the TZHEA is part of the permanent agenda of the regional councils, which may form task teams to work on the TZHEA at the council level.	+ Advise on changes to the TZHEA based on the architecture standards and changes to the requirements. + Monitor implementation and compliance of digital health investments in accordance with the TZHEA at the council level.

			+ Report monthly, quarterly, and annually to the TZHEA Subcommittee through the NDHS on the progress of and compliance with the TZHEA implementation.

Abbreviations: APHFTA; Association of Private Health Facilities in Tanzania; BAKWATA = Baraza Kuu la Waislamu Tanzania; CEO = Chief Executive Officer; CHMT = council health management team; DICT = Division of Information and Communication Technology DPG = Development Partners' Group; e-GA = e-Government Authority; EA = enterprise architecture; GoT = Government of Tanzania; ICT = information and communication technology; M&E = monitoring and evaluation; MoFP, Ministry of Finance and Planning; MoHCDGEC = Ministry of Health, Community Development, Gender, Elderly and Children; MoWTC = Ministry of Works, Transport and Communications; NDHS = National Digital Health Secretariat; NDHSC = National Digital Health Steering Committee; POPSM&GG President's Office–Public Service Management and Good Governance; PS = Permanent Secretary; PSH = Permanent Secretary for Health; RHMT = regional health management team; SWAp = sector-wide approach; TWG = Technical Working Group; TZHEA = Tanzania Health Enterprise Architecture; JAHSR = joint annual health sector review; FBO = faith-based organization.

9.3 TZHEA change-management process

A change-management process can ensure that TZHEA standards and guidelines achieve the intended benefits. It includes managing changes to the standards and guidelines in a cohesive and structured way to support a dynamic environment.

The process typically provides for the continual monitoring of new developments in technology and changes in the business environment, and it helps determine whether and when to formally initiate updates to the standards and guidelines. The change-management process for the TZHEA must include how to manage changes, what techniques to apply, and what methodologies to use.

Table 36 lists key drivers of change that will require management.

Table 36. Key drivers of change.

Business drivers	Technology drivers
+ Developments and evolution in the health sector or government operations. + Exceptions in the health sector or government operations. + Innovations in the health sector or government services. + Strategic changes in the eHealth or e-Government strategic plan.	+ New technologies available for the health sector or government. + Asset-management cost-reduction initiatives undertaken by the health sector or government. + Initiatives to standardize the technology platform for the health sector or government. + Innovations in technology—eHealth or e-Government.

Changes to the TZHEA will fall into one of three categories: simplification, incremental, or re-architecting. Before implementing a review or change, it is crucial to categorize the change and plan for appropriate actions and activities. Table 37 describes the three categories.

Table 37. Categories of changes to the Tanzania Health Enterprise Architecture.

Change category	Description	Extent of change impact
Simplification	A simplification change can normally be handled using change-management techniques.	+ The change affects only one stakeholder. + The change was made by special request. + The change may result from the consolidation of multiple systems.
Incremental	An incremental change may be handled using change-management techniques.	+ The changes in technology or standards lead to updates in the technology architecture but not the standards and guidelines.
Re-architecting	A re-architecting change requires putting the related standards and guidelines through the architecture development cycle (revising all	+ The change affects two or more stakeholders.

	affected domains: business, data, application, and/or technology).	+ The change is a significant change in the eHealth strategy.

To determine whether a change falls into the simplification, incremental, or re-architecting category, the following activities should be undertaken:

1. ***Registration of all events that may affect the standards and guidelines.***
2. ***Resource allocation and management for each task to be performed.***
3. ***Assessment of what actions should be taken.***
4. ***Evaluation of the impact of the change.***

9.3.1 TZHEA change-management flow

The change-management flow for the TZHEA's standards and guidelines are depicted in Table 38.

Table 38. Change-management flow for TZHEA standards and guidelines.

Activity	Details
1. Monitor TZHEA implementation	+ Monitor technology and business changes that could affect the TZHEA standards and guidelines. + Monitor the level of adoption of standards and guidelines for the health sector.
2. Identify need for change	+ Assess compliance of current digital health solutions. + Assess change requests and reporting to ensure compliance with the TZHEA, and ensure that expected benefits are being achieved. + Ensure that change-management requests adhere to the defined standards and guidelines.
3. Establish purpose of change and outcome	+ Influence health-sector initiatives to optimize standards and guidelines to achieve the most impact. + Engage TZHEA stakeholders in discussing the purpose of the change, and document requirements and the scope of work.

4. Manage risks	+ Manage risks and provide recommendations for aligning with standards and guidelines.
5. Develop Request for Change to meet performance targets and service levels	+ Make recommendations on the change required to meet performance targets by developing a Request for Change.
6. Manage governance process	+ Conduct meetings to analyze change requests. + Approve or reject change requests.
7. Activate the process to implement the change	+ Produce a request for funding and for updating the standards and guidelines to NDHSC. + Ensure that the changes implemented are captured and documented in the standards and guidelines.

Abbreviations: NDHSC = National Digital Health Steering Committee; TZHEA = Tanzania Health Enterprise Architecture.

9.4 TZHEA implementation

The key activities to be undertaken in implementing the TZHEA are as follows:

1. ***Institutionalize the TZHEA governance structure.***
   + The Permanent Secretary – MoHCDGEC should appoint TZHEA Subcommittee members in consultation with the ICT and M&E TWG chairpersons. The ICT and M&E TWG should provide guidance and stewardship to the committee through monitoring of committee activities and reports.
2. ***Develop a TZHEA health-sector training strategy.***
   + Assess training needs and define the TZHEA health-sector training strategy for capacity-building across various levels.
   + Develop a capacity-building program for the TZHEA.
3. ***Implement a compliance-management process.***
   + The TZHEA Subcommittee should institutionalize TZHEA standards and the guidelines review, monitoring, and compliance processes to ensure adherence of health-sector stakeholders' applications with the TZHEA standards and guidelines.

4. ***Implement an architecture change-management process.***
   + The TZHEA Subcommittee and the ICT and M&E TWG should formalize an architecture change-management process that will handle changes and enhancements to the TZHEA standards and guidelines.
5. ***Implement the TZEA.***
   The TZHEA Subcommittee should:
   + Disseminate the TZHEA guidelines and standards.
   + Review existing processes, tools, and systems and provide recommendations for improvement.
   + Develop the TZHEA road map and migration plan.
   + Review current digital health solutions for compliance with the TZHEA standards and guidelines and make recommendations for improvements.
   + Monitor changes in health-sector goals, strategies, requirements, and priorities in relation to TZHEA implementation requirements.

9.4.1 TZHEA governance standards and technical guidelines

The TZHEA Subcommittee is responsible for developing TZHEA standards and guidelines, to be approved by the NDHSC.

9.4.2 Formalization of TZHEA governance structure and processes

1. The proposed TZHEA governance structure will take effect once the TZHEA blueprint is approved by the MoHCDGEC's Permanent Secretary.
2. The TZHEA governance structure is subject to review at least once every three years.
3. Any exceptions to compliance with the TZHEA governance structure and blueprint should be approved in writing by the chairperson of the NDHSC.

Appendix A. Terms of reference for the Tanzania Health Enterprise Architecture Subcommittee

Background

The Tanzania Health Enterprise Architecture (TZHEA) Subcommittee is an arm of the Information and Communication Technology (ICT) and Monitoring and Evaluation (M&E) Technical Working Group (TWG), which is partly responsible for coordinating, implementing, managing, and monitoring the implementation of the TZHEA.

The subcommittee comprises technical experts in the fields of ICT and leadership from the Ministry of Health, Community Development, Gender, Elderly and Children (MoHCDGEC); President's Office–Regional Administration and Local Government (PORALG); Prime Minister's Office (PMO); Ministry of Finance and Planning; Ministry of Works, Transport and Communications; Tanzania Communication Regulatory Authority; the e-Government Authority; and appointed representatives from development and implementing partners who provide technical advice.

Responsibilities

The TZHEA Subcommittee has the following responsibilities:

1. Recommend digital health solutions to be implemented in the country according to the TZHEA blueprint recommendations.
2. Provide technical support for implementation of digital health activities and solutions to ensure compliance and adherence to TZHEA standards and guidelines.
3. Facilitate enforcement and compliance of digital health standards and guidelines as outlined in the TZHEA blueprint and using the endorsed compliance assessment tools.
4. Provide technical support at the national level to regional referral hospital management teams, regional health management teams, council health management teams, and other stakeholders on matters related to digital health solutions.
5. Engage stakeholders in implementing the TZHEA.
6. Help the ICT and M&E TWG establish implementation priorities for digital health solutions and coordinate resources needed to implement the TZHEA.

7. Prepare and submit monthly, quarterly, and annual reports on the implementation of the TZHEA to the ICT and M&E TWG, Center for Digital Health, and the Digital Health Steering Committee of the National Digital Health Steering Committee (NDHSC).
8. Help build the capacity of and mentor health-sector stakeholders on the TZHEA.
9. Initiate, manage, and track changes to the TZHEA blueprint to ensure its relevance and applicability, in collaboration with the M&E and ICT TWG, NDHSC, and other stakeholders.

Reporting and accountability

The subcommittee and the chairperson shall be appointed by the Permanent Secretary of the MoHCDGEC after consultation with the ICT and M&E TWG chairpersons. The subcommittee shall submit regular progress reports to the ICT and M&E TWG and the NDHSC.

Membership

The TZHEA shall be chaired by an officer appointed from the Directorate of Curative Services from the MoHCDGEC and shall comprise the following members:

1. Chairperson: Assistant Director, Public and Private Health Services Section, MoHCDGEC.
2. Co-chairperson: Assistant Director, Division of Health Services – Health, PORALG.
3. Secretary: Selected head of section from ICT Unit (should not be Division of Information and Communication Technology), MoHCDGEC.
4. An officer responsible for M&E from the Division of M&E, MoHCDGEC.
5. Appointed officer from the Directorate of Curative Services, MoHCDGEC.
6. Appointed officer from the Directorate of Preventive Services, MoHCDGEC.
7. Appointed officer from the Directorate of Human Resource Development, MoHCDGEC.
8. Assistant Director / officer appointed by the director of ICT department, PORALG.
9. Appointed officer responsible for the TZHEA, e-Government Authority.
10. Appointed officer with responsibility for communication, Ministry of Works, Transport and Communications.
11. Appointed officer responsible for sector coordination, PMO.
12. Appointed officer responsible for planning, Ministry of Finance and Planning.
13. Appointed officer responsible for enterprise architecture and security, Tanzania Communications Regulatory Authority.
14. Advisor: representative of implementing partners.

Meetings

+ The subcommittee shall meet once every two months.
+ Meetings may be conducted face to face or virtually.
+ Ad hoc meetings may be initiated by the chairpersons after consultation with the secretary.
+ Quorum for the meeting shall be seven members.

References

[i] World Health Organization (WHO). *Management of Patient Information: Trends and Challenges in Member States*. Geneva: WHO; 2012. https://apps.who.int/iris/bitstream/handle/10665/76794/9789241504645_eng.pdf;jsessionid=149792348A30C6FC1E23747ED153EC46?sequence=1. Global Observatory for eHealth Series, Vol. 6.

[ii] The Open Group website. The TOGAF® Standard, version 9.2 overview page. https://www.opengroup.org/togaf-standard-version-92-overview. Accessed 20 May 2019.

[iii] President's Office–Public Service Management, e-Government Authority (e-GA). *e-Government Business Architecture – Standards and Technical Guidelines: Document Number eGA/EXT/BSA/001*. Dar es Salaam: e-GA; November 2017. https://www.ega.go.tz/uploads/standards/en-1574936559-business.pdf.

[iv] President's Office–Public Service Management, e-Government Authority (e-GA). *e-Government Information Architecture – Standards and Technical Guidelines: Document Number eGA/EXT/IFA/001*. Dar es Salaam: e-GA; November 2017. https://www.ega.go.tz/uploads/standards/en-1574944904-info.pdf.

[v] President's Office–Public Service Management, e-Government Authority (e-GA). *e-Government Infrastructure Architecture – Standards and Technical Guidelines: Document Number eGA/EXT/IRA/001*. Dar es Salaam: e-GA; November 2017. https://www.ega.go.tz/uploads/standards/en-1574945177-infrast.pdf.

[vi] President's Office–Public Service Management, e-Government Authority (e-GA). *e-Government Interoperability Framework – Standards and Technical Guidelines (e-GIF): Document Number eGA/EXT/GIF/001*. Dar es Salaam: e-GA; February 2016. https://www.ega.go.tz/uploads/standards/en-1574945623-inter.pdf.

[vii] President's Office–Public Service Management, e-Government Authority (e-GA). *e-Government Security Architecture – Standards and Technical Guidelines: Document Number eGA/EXT/ISA/001*. Dar es Salaam: e-GA; November 2017. https://www.ega.go.tz/uploads/standards/en-1574945979-secac.pdf.

[viii] President's Office–Public Service Management, e-Government Authority (e-GA). *e-Government Integration Architecture – Standards and Technical Guidelines:*

Document Number eGA/EXT/ITA/001. Dar es Salaam: e-GA; November 2017. https://www.ega.go.tz/uploads/standards/en-1574946787-GRATION.pdf.

[ix] President's Office–Public Service Management, e-Government Authority (e-GA). *e-Government Architecture Processes and Governance – Standards and Technical Guidelines: Document Number eGA/EXT/PAG/001*. Dar es Salaam: eGA; November 2017. https://www.ega.go.tz/uploads/standards/en-1574947079-PROCESS%20DOC.pdf.

[x] President's Office–Public Service Management, e-Government Authority (e-GA). *National Health Policy*. Dar es Salaam: e-GA; 2019.

[xi] President's Office–Public Service Management, e-Government Authority (e-GA). *Health Sector Strategic Plan IV*. Dar es Salaam: e-GA. http://hidl.afya.go.tz/#/library/dashboard/document-details/25.

[xii] James G, Friedman T. *Enterprise Data Architecture: Why, What and How* [research note]. Stamford, CT: Gartner; 2003.

[xiii] President's Office–Public Service Management, e-Government Authority (e-GA). *e-Government Application Architecture – Standards and Technical Guidelines: Document Number eGA/EXT/APA/001*. Dar es Salaam: e-GA; November 2017. https://www.ega.go.tz/uploads/standards/en-1574925310-apps%20archt.pdf.

UNITED REPUBLIC OF TANZANIA

Ministry of Health, Community Development, Gender, Elderly and Children

Visit:
www.moh.go.tz