Sri Lanka Digital Health Blueprint

Version 1.0 Final

Enabling a healthier Nation through Digital transformation of healthcare

Ministry of Health

Executive Summary

Health information is one of the key pillars of health system. The Health Information System (HIS) revolutionized the method of information usage for decision making. A HIS encompasses all health data sources required by a country for the provision of healthcare and to plan, implement, monitor, and evaluate its national health strategies and action plans.

There were many obstacles identified due to the use of paper-based health information systems, such as the unavailability of real time data, lack of readily accessible and poor quality of data which affects timely informed decision making. Therefore, the Ministry of Health has identified that the digitalization of health services, including the incorporation of the health information system, is a fundamental need to improve quality and effectiveness of the health care delivery in the country.

The digitalization of healthcare in Sri Lanka was initiated at the beginning of the second decade of the 21st century. The digital transformation is related to governance, clinical care, public health, education, and health administration. The adoption of Health Informatics as a specialty field of medicine has accelerated the digital transition of the health system in Sri Lanka. The digital transformation included various information systems, including hospital health information systems, public health information systems, statistical health information systems, and logistic/human resource systems. More than 85 major state sector hospitals have been empowered with the two leading hospital health information systems (HHIMS and HIMS) and more than 12 million patients have registered. These hospital information systems cover outpatient departments, admissions, clinics, transfers, and discharges, as well as laboratory, pharmacy, radiology, and appointment booking information.

This Sri Lanka Digital Health Blueprint (DHB) defines the path that the Ministry of Health, should take in transforming digital health. This process will streamline the digitalization of the health sector in Sri Lanka, optimizing scarce resources at a time of financial constraint.

The Blueprint proposes a National Electronic Health Record (NeHR) as one of its central components. The NeHR will serve as a lifelong record of individual patients from birth to death. It has also been identified that the interoperability of systems and information sharing are key to the success of digital health systems and their use. The digital health platform specified and detailed in this Digital Health Blueprint, will form the basis for delivering the above components and functions. Other deliverables include point-of-care services, central registries, centralized services, document repositories, a data warehouse, authentication services, audit trails, information dashboards, and a national health data exchange.

The realisation of the Blueprint will be pragmatically phased out to ensure focused mobilisation of the resources available and sustainability of the systems implemented. The Ministry also plans to improve the required human resource capacity to support this endeavour. All the future investment on digital health should be align with Digitl Health Blueprint and implementation roadmap.

I wish to thank everyone involved in developing the Sri Lanka Digital Health Blueprint, specially the Health Information Unit of the Ministry of Health, for their untiring efforts. I hope Digitl Health Blueprint will undergo necessary modifications and updates as and when required with advancing technology.

Dr. Palitha Karunapema
Director Health Information,
Ministry of Health.

Message from the Secretary of Health

The National Health Policy 2016–2025 outlines a robust framework for achieving national health goals, including Sustainable Development Goals (SGDs), through the adoption of the basic principles of accessibility, quality, and affordability and by leveraging the power of information and communication technologies to strengthen health care delivery systems.

Digital health interventions strengthen and support the outcomes of every health service delivery programme in the country. With increased ease of use, acceptance by the masses, and adaptation by service providers, digital health interventions can be a powerful instrument in accelerating the transformation of the health agenda and enhancing the health outcomes of the entire population of the nation. The integration of many digital interventions in the ecosystem of digital health is essential for a holistic pursuit of the goals of National Health Policy 2016-2025 and the SDGs relating to health. The Ministry of health has initiated efforts for establishing a comprehensive, integrated Digital Health ecosystem through an architectural framework namely, the Digital Health Blueprint (DHB) in line with Government overall digital transformation framework.

I appreciate the efforts of the Health Information Unit of the Ministry of Health, all the relevant stakeholders including Director General of Health Services, all the deputy director generals, directors and deputy directors of the Ministry of Health, Information Communication Technology Agency, the Global Fund, WHO and other international partners in developing Sri Lanka Digital Health Blueprint. I request all the stakeholders to put this plan into action and create the conditions necessary for Sri Lanka to become a nation that is a leader in digital healthcare and improve health outcome of the population.

Mr. S. Janaka Sri Chandraguptha
Secretary / Ministry of Health

Message from the Director General of Health Services

Global evidence shows the digitalization of the health information system has made it feasible to take a significant step toward establishing universal health care.

The Ministry of Health of Sri Lanka has demonstrated the use of digital health interventions in major national health programs, which have benefited patients with timely service delivery and made government healthcare services more efficient and accessible.

However, all these efforts need to converge into a single framework to achieve interoperability of data, which would benefit both policymakers for decision making and patients with effective services at the time of need. The Sri Lanka Digital Health Blueprint provides clear guidance for all stakeholders to engage and contribute to strengthening the digital health system in Sri Lanka.

I would like to specially acknowledge and thank the Management Development and Planning Unit of the Ministry of Health, Information Communication Technology Agency, the Global Fund, and all the other stakeholders, including the medical specialty of Health Informatics, for initiating the development of the National Digital Health Blueprint for Sri Lanka and the digital transformation of the health sector.

The Ministry of Health is dedicated to taking all necessary actions to ensure that the Digital Health Blueprint is successfully implemented throughout the entire health sector.

Dr. Asela Gunawardena
Director General of Health Services

Message from the Deputy Director General-Planning

Information is a key building block of any health system. Information is required for day-to-day clinical decisions, planning, and administration purposes. Evidence-based decision making is very important in healthcare. Globally, healthcare systems are adopting digital systems, processors, and tools to enhance the function of health information systems.

Digital health information systems can provide relevant data to clinicians as well as health administrators for decision making purposes. Relevant, accurate, complete, and timely information supports health planning, strategizing, making policy decisions and research. Information is vital in planning for the development of infrastructure, human resource capacity building, and financing for the long term and sustainability.

It is important that all digital health initiatives are properly coordinated by the Health Information Unit of the Ministry, in line with the Digitl Health Bueprint. All digital health initiatives and investment should be aligned with DHPB to improve cohesiveness, avoid duplication of efforts, and better utilize our limited resources.

The Sri Lanka Digital Health Blueprint will serve as a guide for achieving all these goals and subsequently raising the standard of healthcare in Sri Lanka.

Dr. S. Sridharan
Deputy Director General- Planning
Ministry of Health

Table of Figures

Table of Contents

I. Foreward

The 2016-2025 National Health Strategic Master Plan of Sri Lanka identified the need for a formalised health information management programme, to be led by a Director of Health Information. The plan recognised the limits of the traditional information flow and its impact on decision making and policy creation. The plan highlighted the many benefits of a digital health approach, including improved efficiency, safety, and long-term cost benefits.

According to the plan, the primary beneficiaries of the National Digital Health Policies of Sri Lanka are stated to be:

- Patients seeking care at healthcare institutions
- Providers during healthcare delivery processes and using clinical decision support
- Public health officials utilising disease monitoring data
- Citizens utilising health services
- Health Administrators utilising data to make evidence-based decisions and policies
- Digital health vendors investing in new digital health platforms
- Health related software developers to recognize digital health architecture

While efforts to develop and deploy digital health technology have been widespread across Sri Lanka, the benefits have been quite localised, and exchange of individual patient data is limited. A citizen cannot access his or her health records, clinicians order and undertake diagnostic tests without insight into other activities in other disease verticals, and what solutions do exist create isolated medical records. This can create increased burden on citizens to ensure they appropriately seek care and inform medical providers of their history.

The Health Information Unit at the Ministry of Health (HIU) Sri Lanka, the Information and Communication Technology Agency (ICTA) of Sri Lanka, and other stakeholders have coordinated to engage with stakeholder groups and have developed several artefacts to foster interoperable and interconnected digital health solutions. Including:

- The Digital Health Enterprise Architecture Plan (DHEAP)
- The National Digital Health Guidelines and Standards (NDHGS)
- Current State Assessment Documentation

With this background information collected and requirements being documented, the Ministry of Heath, TWG BluePHIE stakeholders, ICTA, and international agencies have undertaken the development of the Sri Lanka Digital Health Blueprint contained herewith.

This blueprint was developed with the engagement of various stakeholder's groups within Sri Lanka including the consultant Health informaticians as the main medical spciality related to Digital Health and is based on a variety of international best practices, blueprints, and standards. In addition to the existing artefacts produced within Sri Lanka, other sources of inspiration for this document and the architecture it describes include:

- The Digital Health Blueprint of India
- WHO-ITU Digital Health Platform Handbook
- Open Health Information Exchange (OpenHIE)
- Canada Health Infoway's e-Health Blueprint v2
- Integrating the Healthcare Enterprise (IHE) architectural patterns such as: Cross Community Access (XCA) and Cross Community Document Exchange for Imaging (XDS-I)
- HL7 Standards

The blueprint represents an architectural vision for an interconnected and interoperable digital health ecosystem within Sri Lanka. The blueprint document includes details only about the information systems that were explained in detail by the heads of the institutes to the HIU and the ICTA. Any Information system that functions independently and has not been divulged to the HIU during the time of assessment has not been considered in this version of the blueprint, however, the blueprint is designed to be inclusive and to evolve over time to eventually include all systems of strategic value. The blueprint seeks to be software and implementation agnostic, while establishing patterns of interchange, descriptions of foundational business services, and a framework for further specification of information interchange within Sri Lanka. The key features of the blueprint are:

- A set of overall architectural, business, information, and functional principles that can be used to guide a cost-effective evolutionary path from the existing digital environment to the future state,
- A modern services-oriented architecture (SOA) based design pattern,
- A common pattern and framework for realising the architecture (via its architectural views, and realisation plan),
- Registries for unique identification of subjects of care (referred to as clients or patients in this document), providers of care (organisations, and workers), supplies (drugs, devices, and materials), and facilities (locations, hospitals, and clinics),
- A National Electronic Health Record (NEHR) providing a lifetime view of summary information for patients,
- Enterprise single sign on of application API keys and users,
- Security and privacy by design,
- National Digital Health Information Warehouse for administrative planning, public health, and evidence-based research purposes.

The blueprint should not be seen as a detailed software architecture specification which prescribes how software is developed. Rather, the blueprint proposes a conceptual, informative structure within which technological solutions are realised, and by doing so, allows for flexibility of the blueprint to scale within a heterogenous software environment functionally, administratively, geographically, and generationally.

The Sri Lanka Digital Health Blueprint organises existing artefacts (the DHEAP, NDHGS, application architecture, solution requirements documents, and others) and builds upon them, presenting a common framework for a nationally scoped digital health ecosystem within Sri Lanka. By doing so, the blueprint can be realised in an evolutionary manner over the coming decade.

The authors of the blueprint would like to acknowledge the commitment and contributions made by our key stakeholder groups in the development of this document, and in their commitment to continual development and improvement of the blueprint and digital health ecosystem, for the benefit of all Sri Lankan by expansion of health services through digital health modalities.

This is the first version of the Digital Health Blueprint; future versions of the blueprint will be published after in-depth consultation with stakeholders.

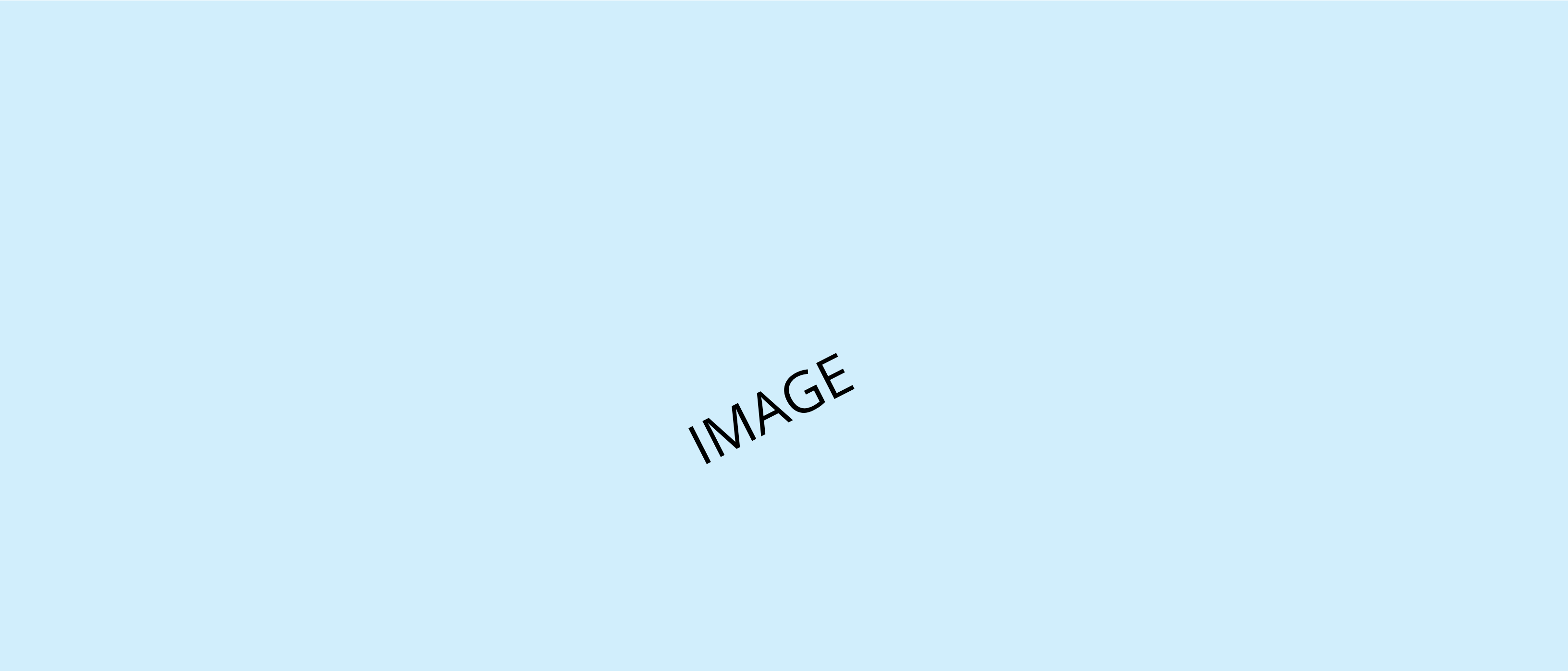
11.1 Glossary of Terms

Term	Definition
DHBP	Sri Lanka Digital Health Blueprint (see: 2.4.1)
DHP	Digital Health Platform (see: 2.4.4)
DHS	Digital Health Service (see: 2.4.3)
NEHR	National Electronic Health Record (see: 2.4.2)
MPI	Master Patient Index – A solution which is responsible for maintaining and cross referencing the identity of persons/patients within the authority.
MoH	Ministry of Health
API	Application Programming Interface – in the context of the digital health blueprint, the term API is used to describe a business goal or operation as opposed to a specific technology implementation (ex. function call, HTTP, REST, etc.)
Client / Patient	The term Client and Patient are used interchangeably in this document and are used to describe an individual who is seeking or being provided care by the Sri Lankan Health System (public or private, curative or preventative).
Provider	Refers to an individual who is providing care to a client within the health system. Examples of providers include medical officers, private medical institutions, nurses, etc.
SOA	Services Oriented Architecture – describes a pattern of enterprise application integration whereby individual services (such as APIs) are consumed, orchestrated, and governed to achieve an enterprise business goal.
REST	Representational State Transfer – described a pattern of data exchange where a sending system serialises a data structure (a resource) to a wire format and shares this data with another system over the HTTP protocol.
FHIR	Fast Health Interoperability Resources – A resource-based interoperability standard which defines a common format for representing health resources, as well as related processes for specification, validation, and transport.
HL7	Health Level 7 – An ANSI accredited standards development organisation which specifies and governs the development of a variety of standards.
ICD	International Classification of Disease – An international standard maintained by the World Health Organization which is used to represent clinical concepts in a computable manner.
SNOMED	Systematized Nomenclature of Medicine – An international standard maintained by IHTSDO which is used to present complex clinical concepts in a structured ontology.
LOINC	Logical Observation Identifiers Names and Codes – An international standard maintained by the Regenstrief Institute which is used to codify observation classifications and results.
IHE	Integrating the Healthcare Enterprise – An international profiling organisation which provides concrete implementation patterns, data exchange specifications, and inter-standard considerations for health information exchange.

DICOM	Digital Imaging and Communications in Medicine – An interoperability standard primarily concerned with the exchange, capture, and processing of diagnostic images to/from PACS solutions.
WADO	Web Access to DICOM Objects – A web-enabled wrapper for DICOM which allows for accession of DICOM objects in a RIS or PACS.
QIDO	Query Based on ID for DICOM Objects – A REST based wrapper for accessing DICOM object using their identifiers.
RIS	Radiology Information System
PACS	Picture Archiving and Communications System
OAUTH	Open Authentication – An interoperability standard primarily concerned with the authentication of users of transport of authentication tokens.
OpenID	Open Identity – A specification (restriction) built on OAUTH which standardises the methods and tokens used for accessing protected resources using REST APIs.
HTTP	Hypertext Transfer Protocol
NeHSC	National e-Health Steering Committee
LGC	Lanka Government Cloud – A shared government cloud environment which is used for digital government services provided in Sri Lanka. The goal of the LGC is to reduce cost and foster reuse of technical assets.
LGN	Lanka Government Network – A network which provides a virtual private connection for government services.
NDX	National Data Exchange – An API gateway which provides mediation between systems in use in Sri Lanka
NHDX	National Health Data Exchange – An API gateway and service bus implemented on the base of the NDX for sharing health information.
COTS	Common Off the Shelf – Indicates that software or services are purchased and configured rather than developed in-house (for example: Open Office, Word, XenDesk, etc.)
ICTA	Information Communications Technology Agency – An agency of the government of Sri Lanka which is responsible for the implementation of all ICT projects initiated by the government.
PHI	Personal Health Information – Discrete health information stored about a person’s interactions with the health system which is directly identifiable to the individual.
Healthcare Institution	Any State or Private Institute in Sri Lanka which provides curative or preventive health care services
KPI	Key Performance Indicator
PMI	Private Medical Institution – A setting in the private health system where curative or preventative services are delivered.
MCDS	Minimum Clinical Data Set
RPO	Recovery Point Objective

RTO	Recovery Time Objective
MTO	Maximum Tolerable Outage
SIEM	Security Information Event Management – Software which is used by operators of infrastructure to monitor the events generated by servers and networks. This is often used to detect and protect infrastructure.
APM	Application Performance Monitoring – Software which evaluates the performance of various services and technologies on virtualised infrastructure. APM can be used to measure and detect performance degradation, application-level issues, or database issues.

11.2 Document Licence & Copyright Notices



1. Background & Context

The Democratic Socialist Republic of Sri Lanka, previously known as Ceylon, is an island nation approximately 65,000km^2 situated in the Indian Ocean. With a GDP of $3,682 per capita, Sri Lanka is a lower middle-income country which has a population of 21.9 million people.

Sri Lanka provides free healthcare to all its citizens. Government expenditure on Health was approximately 4.08% of GDP in 2019[1] and, despite the relatively low expenditure the country's health indicators have been on par with countries in the region.

Sri Lankans can seek care from many different practices within the country, however the allopathic system caters to the needs of most of the population via private and public delivery, with very minor additional services provided by non-profit organisations.

The bulk of the inpatient burden of care in Sri Lanka (95%) and about half (50%) of outpatient care services are provided by the public sector[2], which handled more than 6 million hospitalisations and over 55 million outpatient visits in 2017[3].

[1] Sri Lanka Healthcare Spending 2000-2022 | MacroTrends

[2] 9789290228530-eng.pdf (who.int)

[3] www.health.gov.lk/moh_final/english/public/elfinder/files/publications/AHB/2020/AHB_2017.pdf

The government health sector comprises of following key streams:

- Curative Care: Delivery of non-specialised primary care and specialised tertiary care through a network of care institutions throughout the country.
- Preventative Care: Delivery of community health services which focus on disease prevention, the promotion of health and early interventions.

Each of the streams mentioned above also provides Capacity Building, such as undergraduate supportive hospital base training and full time In-service training of health professionals. They also provide Supportive Services, such as aiding with logistics, drugs, equipment, and medical devices.

The delivery of care in the public system is provided by over 1,600 institutions (consisting of hospitals, primary care units, and preventative care institutes) of which 641 are hospitals operated by the central government and provinces (provincial council hospitals). On average, the availability of hospital services is 3.5 beds per 1,000 persons. Community care is provided through 354 medical officer of health divisions across the country provide community care. Training of undergraduate medical students and paramedical students done by the teaching hospitals. Also Inservice training of some paramedical students is done by training schools joined to teaching hospitals.

Currently there are 91 medical officers and 212.4 nursing staff per 100,000 persons[4].

1.1 Health System Organisation

The Sri Lanka Health System Review produced by the Asia Pacific Observatory on Health Systems and Policies[2] provides an in-depth view of the organisational structure of the ministry of health. This content is summarised in this document for convenience of the reader.

The key agency for health services is the Ministry of Health (MOH) of the government of Sri Lanka. The Ministry is responsible for policy development, regulatory functions, resource allocation, medical supplies, and infrastructure development of the public health sector. The Ministry is headed by a Minister of Health and a Secretary of Health. The Director General of Health Services (DGHS) is the technical head of the department of health and is supported by multiple Deputy Directors General (DDGs) who are mostly specialist administrators or specialist community physicians. There are multiple units under these DDGs, headed by directors (examples: Health Promotion Bureau, Quarantine Unit, etc.). Specific technical work is led by the medical specialists in each field supported by the medical officers and other paramedical staff.

There is a department of health service for each province. Provincial councils are permitted to formulate their own legislations called provincial statutes covering the scope of Health in line with national health policies. Health services in the country are provided by central government institutes as well as the nine provincial health ministry institutes. Almost all MOH offices (354) are directed by Provincial health departments. It is also important to note the importance of the contribution of the private sector, which provides more than 50% of primary care in the country.

There are 354 MOH Areas in Sri Lanka, each headed by a Medical Officer responsible for a defined population which, on average, is between 40,000 and 80,000 population.

Human resource pool of the Sri Lankan health system is made up of around 140,000 personnel from different categories working in the curative and preventive sectors. There are many medical specialists that are involved in this process. For

[4] Digital Health Enterprise Architecture Plan (DHEAP) [1] pg 11

example, digital health related activity is the main responsibility of the medical informatics specialty, and in alignment with current global trends, played a main role in the development of this blueprint.

1.2 Healthcare Vision

The National Policy on Health of Sri Lanka[5] states the healthcare vision for the country as "A healthier nation that contributes to its economic, social, mental and spiritual development". The policy identifies eleven guiding principles which serve as the basis of this Blueprint:

- Citizen centric approaches,
- Good governance and transparency,
- Upholding national values of free healthcare, the right to health, universal health coverage and equity and social justice.
- Encouraging multiple stakeholder involvement, collaboration and partnerships for information dissemination and sharing.
- Evidence-based decision making and accountability,
- Ensuring the privacy and security of healthcare recipients,
- Sensitivity towards cultural diversity and social norms,
- Systems approach to health information with a focus on interoperability,
- Minimal data redundancy and capture,
- Conformity to technology relevance, simplicity, cost-effectiveness, and efficient use of information resources, and
- Sustainability of information systems.

The national policy describes a Health Information System (HIS) which facilitates an effective, equitable, economical, and quality service while ensuring privacy and confidentiality of care recipients. The national policy set forth objectives including:

- Ensure that health institutions generate, share, and use timely and quality health information to support organisational management and development.
- Make available systems for personalised and community-based health information management. Enabling the continuous care of recipients who receive care at different level of care Ensure optimal data & information sharing and access to health information in relation to relevant sharable data in health information systems while ensuring ethical considerations and confidentiality of recipients.
- Encourage suitable innovations related to health information management in all information processes while ensuring interoperability.
- Ensure security and integrity of all health data/ information systems
- Ensure sustainability to all health information systems

1.2.1 Key Strategic Goals

The National Health Policy established seven Broad Strategic Directions which were summarised in the Digital Health Enterprise Architecture Plan [1] and are shown in Figure 1, which identifies the following goals:

a) Strengthen Service delivery to achieve preventative health goals

b) Appropriate and accessible high-quality Curative care for all Sri Lankan citizens

c) Promotion of equitable access to quality rehabilitation care

d) Strengthen evidence-based service delivery to support journey along the continuum of care

e) Develop new strategies to reduce Out of Pocket Spending (OOPS) and reduce financial risk

[5] PG 3569 Health Policy (E) (documents.gov.lk)5.

f) To ensure a comprehensive health system through a better restructuring including HRM

g) Develop strategic partnership with all providers of care

1.3 Health Information Systems Challenges

According to the United Nations sustainable development goals[7], physical and mental health and wellbeing are key goals for a nation as well as the world. In any system as complex as the delivery of health care services, there are bound to be challenges all countries, regardless of the level of economic development, however the nature of the challenges may be unique to a country or similar between a group of countries with similar socio-economic backgrounds. Health information system challenges related to information, availability, quality, acceptability, utilisation, efficiency, costs and accountability are discussed here.

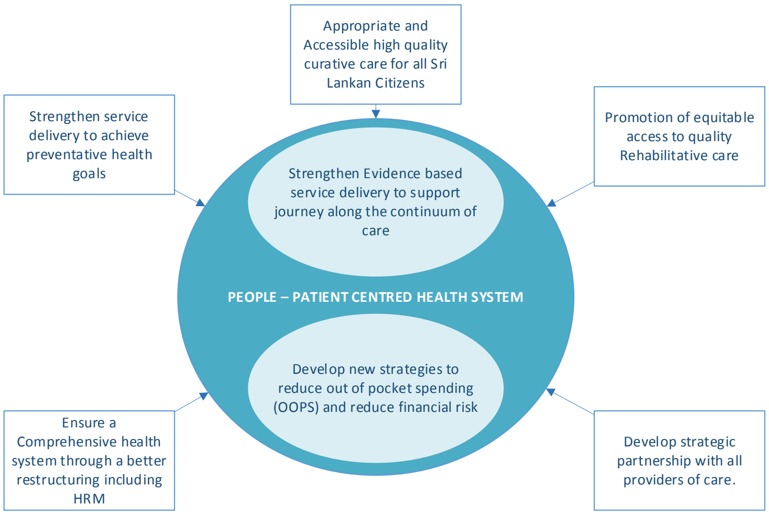

Appropriate and Accessible high quality curative care for all Sri Lankan Citizens
Strengthen service delivery to achieve preventative health goals
Promotion of equitable access to quality Rehabilitative care
Strengthen Evidence based service delivery to support journey along the continuum of care
PEOPLE – PATIENT CENTRED HEALTH SYSTEM
Develop new strategies to reduce out of pocket spending (OOPS) and reduce financial risk
Ensure a Comprehensive health system through a better restructuring including HRM
Develop strategic partnership with all providers of care.

Figure 1 : *Main Strategic Areas of National Health Policy*[6]

Information, and the sharing of it, is a key driver in many business sectors and domains. The lack of availability, or lack of quality, of information in the healthcare sector can be particularly disruptive to streamlined care delivery. In Sri Lanka, digital health solutions have been developed for a variety of care settings (Annex C), however these solutions are localised and are essentially siloed medical records systems. The Blueprint ecosystem was developed based on shared systems details with the HIU.

For example, there are multiple hospital information systems (HIS) in use within Sri Lanka: Hospital Information Management System / SWASTHA (HIMS – mostly used for inpatient hospital stays), Hospital Health Information Management System (HHIMS – mostly used for outpatient clinics, managed by ICTA), and a variety of private sector solutions. Currently, if a patient transfer is required between hospitals using different (or even similar) systems, there is no digital information sharing. Additionally, discharges, referrals to outpatient services, or specialised services are not digitally shared.

This lack of interoperability and sharing currently adds an extra burden of sending/transferring hardcopies of requisitions, records, results, and summaries between institutions, and relies on

[6] Digital Health Enterprise Architecture Plan (DHEAP) 0.6 [1] - Figure 1.4:1
[7] https://sdgs.un.org/goals

patients, guardians, or medical workers to physically move records around and/or remember their own medical history. This lack of efficient sharing impacts the availability of clinical information where patients cannot produce summaries, recall their own history, or are in emergency situations where they are unable to produce this information. This reduces the accuracy of clinical assessments, treatment plan development, and overall decision making, potentially impacting the quality-of-care delivery. This inefficiency is also costly to the health system as it requires duplication of efforts and increased strain on supplies and reduces the overall capacity to deliver care.

Additionally, these digital health solutions are hampered by several equipment and human resourcing challenges. There is often a lack of available redundant computer terminals within hospitals and clinics. This means that hardware failures result in stations and digital services being unavailable for extended periods of time, requiring staff to fall back to paper-based systems. The lack of a trained, onsite human resource person to provide local helpdesk services also means that repairs of equipment and networks often fall to junior staff members when they are available to fix these issues, when components become available.

Quality of care can be measured from differing perspectives. From a patient perspective, the outcome of their personal experience of the overall delivery and acquisition of care services are the primary measures of the quality of their care. Relying on patients to self-manage medical information can reduce the patient's experience as it imparts an information management burden on them. Additionally, a lack of clear or accurate information from the patient can increase medical burden, as tests are repeated, contraindicated medications are unknown, and unnecessarily repeated procedures.

From an administrative perspective, quality of care is typically measured at a macro level with adherence to guidelines, measuring access to services, and assigning additional supportive supervision are important. Currently, there is no adequate measure of adherence to clinical guidelines, policies, and evidence based best practices in Sri Lanka. Additionally, the lack of robust human resourcing systems means that allocation of human resources including transfers of staff between facilities and/or modifying assignments of staff to address deficiencies in clinical quality can be difficult.

The country's Medical Supplies Divisions (MSD) uses a software package (MSMIS) to manage drug supplies between 200 institutions and drug stores within the country. This solution, however, lacks the ability to track of non-drug medical equipment and supplies (such as film for medical imaging, scalpels, and other equipment) which means that these stock supplies can run low, and in rare cases stockout conditions arise.

The inadequate availability of aggregate data also hampers the ability for public health services to make real-time or near-real-time decisions on data submitted. Currently the availability of public health information in Sri Lanka is not directly integrated with clinical information systems, and accessing this information is sometimes difficult. This makes communicable disease surveillance challenging. It also makes the assessment of clinical quality and accessibility challenging, which may hamper administrative decision-making processes.

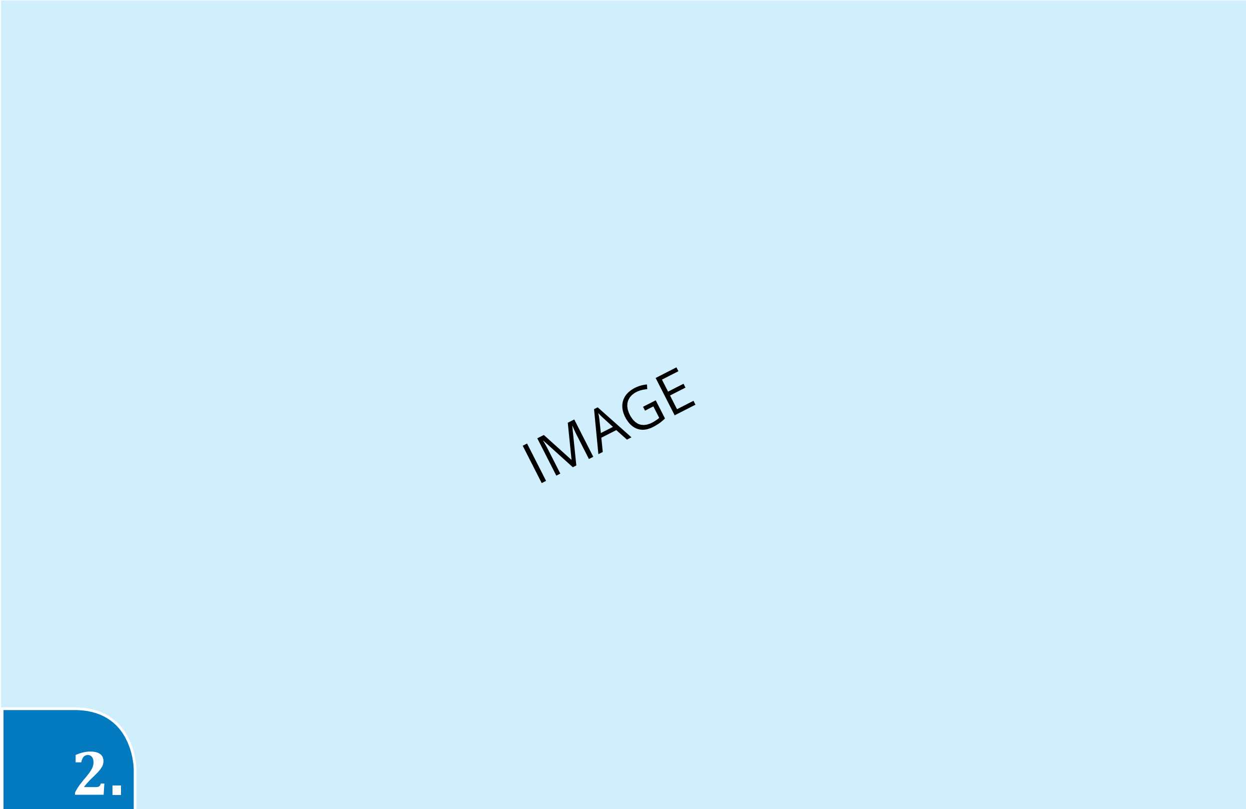
All these issues can lead to a lack of transparency within the health sector. Accountability tracing within the health sector (i.e., staff to the central and provincial Ministries of Health) is difficult, if not impossible with manual processes. Understanding how individual data was disclosed, used, and collected is important for patients and administrators as it can indicate inappropriate use of assets, access of resources, and can provide insights into potential optimisations.

All these challenges can coalesce and manifest in a variety of manners. The poor allocation and utilization of personnel, equipment, consumables, and care settings can lead to increased cost and burden on the central and provincial ministries of health. The lack of clear insight into use of inventory, and health issues can cause understocking or overstocking of materials in facilities. Additionally, the burden of manual aggregate data capture, order and inventory management, and disjointed environments can lead to increased burden on staff, and poorer care.

Implementing stand-alone digital health solutions however is not a panacea. For example, there are already 3 hospital-based health information system currently implemented in healthcare settings which operate individually and do not share information among each other. Public health information systems are also not integrated and do not share information easily.

Further, the current level of digital literacy among health staff and clients is likely inadequate and the capacity to utilise digital health solutions will need to be addressed as the DHP is developed. There are different tiers of digital literacy required depending on the service need, for example operators/ end users of the system, hospital level system administrators, national level administrators, etc.

It is vital to the financial sustainability and viability of the health system that efficient, effective, and appropriate use of health services by staff and patients be realised. Only through robust data capture, sharing, aggregation, and dissemination can this be achieved.



2. Introduction

This section presents the key elements which were considered in establishing the digital health blueprint for Sri Lanka. Most of these elements emanated from the referenced documents (see table II.2), and consultations with Ministry of Health and related stakeholders of Sri Lanka.

2.1 Introducing the Digital Health Blueprint

The most effective manner to resolve the health information system challenges in Sri Lanka, is the adoption of a well-designed, well-connected, and highly available health workforce, and related digital tools to support that workforce.

This adoption is a journey to an ever evolving and changing destination. The blueprint describes a digital health platform which will support the secure and confidential digital health future within Sri Lanka as envisioned within the National Policy on Health[8].

Healthcare is a broad and deep domain, and the wide array of projects currently being undertaken by the Ministry of Health, the Health Information Unit, and ICTA are starting this transformation.

The blueprint sets forth a framework for moving towards a future state and seeks to align the current and future digital health interventions leveraged within Sri Lanka. The alignment of health information resources; indicators and data elements; data and

[8] (documents.gov.lk)

information management practices; information security, privacy, confidentiality, and ethics; and innovation are considered.

The blueprint sets forth a consistent framework for the specification of interchanges between solutions (the principles, views, and concepts of the blueprint), proposing a business service-based architecture, proposing a common architecture for integration using shared services, common information concepts and flows, and technical/ functional principles for digital health solutions in Sri Lanka.

Realisation of the blueprint will require multiple projects to be executed over the coming decades. Broadly speaking, the initial realisation of a digital health future for Sri Lanka involves:

a) **Digitisation** of clinical workflows (such as primary care, inward base care, laboratory, imaging, etc.), public health information, human resourcing and identification, logistics management and more using digital software platforms. This includes the increasing of digital literacy of users leveraging massive, open, online courses (MOOC) for users via e-Learning.
b) **Connecting** those digital health solutions to the broader ecosystem by increasing available infrastructure such as local and wide area networks and cellular infrastructure, increasing access to mobile technologies, and providing workstations capable of participating in this connectivity.
c) **Sharing** information between digital health solutions using open, consistent, and available application programming interfaces (APIs) for the use of clinical curative and preventative delivery as well as administrative planning and monitoring purposes.

Once these baseline activities are completed, and become more broadly available within the country, it then becomes possible to:

d) **Inform** clinical providers and administrators decision-making process via access to the digitised, connected, and shared data.
e) **Innovate** on clinical and administrative processes by using evidence-based approaches based on real data from the digital health infrastructure. The digital health platform by its service-based nature also fosters digital innovations within the public and private sectors.
f) **Transform** the health system of Sri Lanka into a more efficient, quality and patient centric health care delivery system future where data and good decision making are omnipresent via the shared, digital health platform.

2.2 Alignment to Sri Lanka Government Enterprise Architecture (SL-GEA)

The SL-GEA seeks to provide a whole government architectural approach for a digitally inclusive Sri Lanka. The SL-GEA identifies three core values for digital solutions in Sri Lanka, which this blueprint aligns with:

1. *Citizens First* – The blueprint provides a patient centred approach to integration of the Sri Lanka digital health ecosystem.
2. *Government as a Platform* – The blueprint is designed to foster service reusability, providing common services for health information exchange, and a framework for business domain specification.
3. *Empowerment of Government Officers* – The blueprint serves as an enabler of health care providers, and secondary use for health administration and public health purposes.

Throughout the development of the blueprint the stakeholders and involved persons considered the four key strategies identified in the SL-GEA:

- *Citizens and Business Focused Solutions*– By providing a common framework for representing digital health solutions within the broader enterprise aligned to the principles of provider benefit and patient centredness.
- *Shared Digital Services and Platforms* – By providing a definition of common business domains, application concerns and integration between each.
- Developing a Highly Available and Secure System – By treating privacy and security as a service, leveraging a services-oriented architecture (SOA) approach, and defining common IT infrastructure for health services.
- Unified Approach Towards Digital Transformation – By focusing on interoperability and standardisation of technical components and business processes through the solution and technical views of the blueprint framework.

2.3 Architectural Views (Enterprise vs. Logical vs. Technical)

This document specifies the requirements, outline of the structure, as well as major features and components of a digital health platform architecture. It sets out the framework for implementing an interoperable health system using layers of detail expressed in different views.

Figure 2 provides a summary of the levels of specificity of this document and its relationship to other documents which provide further specification of the digital health system in Sri Lanka.

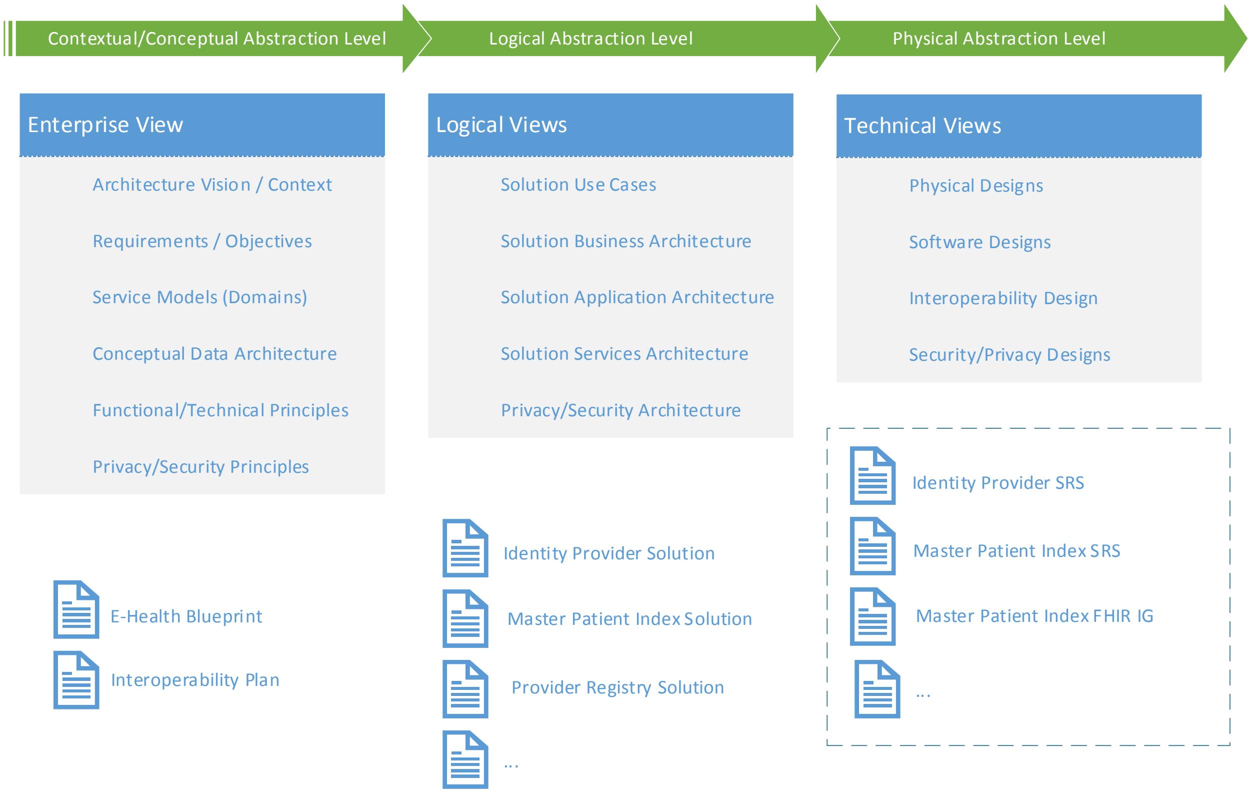

Contextual/Conceptual Abstraction Level
Logical Abstraction Level
Physical Abstraction Level
Enterprise View
Architecture Vision / Context
Requirements / Objectives
Service Models (Domains)
Conceptual Data Architecture
Functional/Technical Principles
Privacy/Security Principles
Logical Views
Solution Use Cases
Solution Business Architecture
Solution Application Architecture
Solution Services Architecture
Privacy/Security Architecture
Technical Views
Physical Designs
Software Designs
Interoperability Design
Security/Privacy Designs
Identity Provider SRS
Master Patient Index SRS
Master Patient Index FHIR IG
...
Identity Provider Solution
Master Patient Index Solution
Provider Registry Solution
...
E-Health Blueprint
Interoperability Plan

Figure 2 : *Architectural Levels and Artefacts*

Each view targets a different scope within the enterprise design, and audience. Table 1 provides a summary of the audience and scope for each view.

Table 1 – Audience and Scope

View	***Audience***	***Scope***	***Detail***
Enterprise View	All stakeholders	National/Provincial	Low
Logical View	Business Owners	National/Provincial	Moderate
Technical View	Operators and Developers	System/Application	High

2.3.1 Enterprise View

The enterprise view of the Sri Lankan digital heath architecture is primarily concerned with the conceptual views, frameworks, patterns, principles, and concepts upon which digital health services in Sri Lanka will be implemented and integrated.

The enterprise view of the Sri Lanka Digital Health Blueprint is comprised of two key documents used to disseminate the vision to relevant stakeholders:

- Digital Health Blueprint: This document, which describes the overall conceptual business, information and application architectures, governing principals, vision and general realisation plan.

National Interoperability Plan: This document describes the structure, processes and cross-domain considerations for developing interoperability profiles within the Sri Lanka context and serves as guidance on the implementation of the interoperability in Sri Lanka.

2.3.2 Logical Views

While the enterprise view is a high-level document which focuses on common patterns and structure between enterprise services and processes, logical views are intended to provide deeper analysis of the design of a particular component (for example: Master Patient Index, Terminology Service, or Provider Registry) and its interdependencies.

The logical views are intended to facilitate the attainment of interoperability between systems for a particular enterprise component. These logical views contain interoperability profiles of relevant international standards, business triggers for sending data, security considerations, and the obligations of both providers and consumers of digital health services.

For example, the Master Patient Index will be realised as a software system, however there are potentially dozens of software solutions which must interact with this service. The logical view informs both the design of the provider of the service (in the example, the Master Patient Index), as well as consumers of the service (hospital systems, EMRs, etc.) of the overall use case and flow of information within a particular domain.

2.3.3 Technical View

The next level of detail which is required to realise the digital health blueprint of Sri Lanka are technical views. These documents are primarily authored to assist implementers (such as developers, operations staff, and users) integrate and implement the blueprint in a physical realisation.

Each domain may have one or more technical views representing the implementation of the logical enterprise component and expresses the data structures, APIs and transactions, and software considerations within a particular implementation technology. These may manifest as API documentation, FHIR implementation guides, or other structures appropriate for the implementation technology.

2.3.4 Enterprise Architecture Frameworks

The development of this blueprint takes inspiration from several enterprise architecture frameworks. The most notable of which are the Federal Enterprise Architecture Framework (FEAF)[9] and The Open Group Architecture Framework (TOGAF)[10]. Furthermore, the blueprint draws inspiration for design elements and structure from Canada Health Infoway's Blueprint[11], OpenHIE[12], the National Health Blueprint of India[13], Integrating the Healthcare Enterprise[14], and WHO-ITU Digital Health Platform Handbook[15].

In this document, the health enterprise is separated into conceptual business domains which contain one or more conceptual business services. It is envisioned that these business services will be described and specified further in solution and technical views. This strategy allows the blueprint architecture to be decomposed into more consumable pieces and implemented over time.

2.4 Key Definitions & Overarching Concepts

The purpose of the digital health blueprint is to provide a framework for the consistent planning for the design and implementation of shared digital health services within Sri Lanka.

This section provides essential information about the key definitions and concepts of this blueprint document which will assist readers and implementers in the understanding of how this document relates to others in the Sri Lanka health enterprise. Figure 3 illustrates the relationship between these concepts.

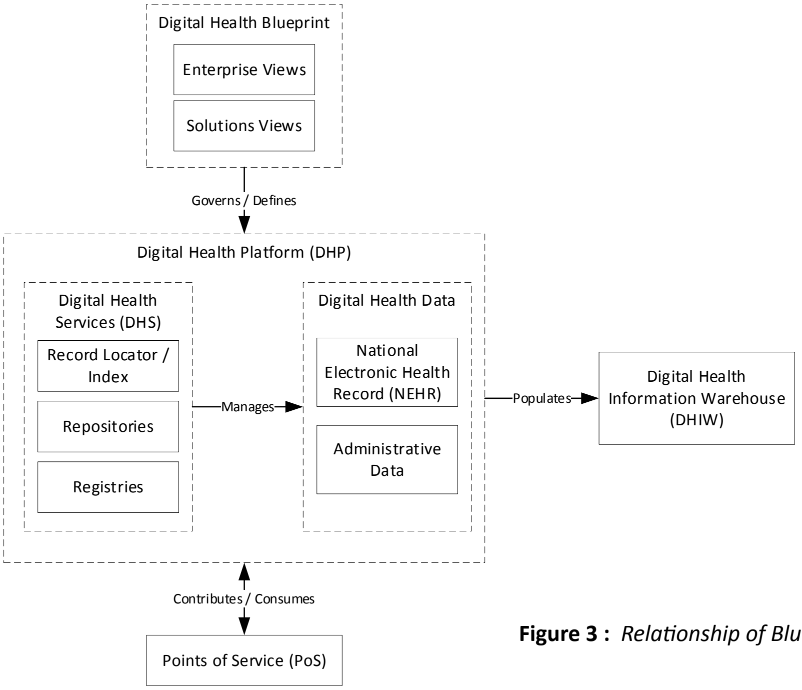


Figure 3 : *Relationship of Blueprint Concepts*

[9] U.S. Cloud Computing Strategy (archives.gov)
[10] TOGAF | The Open Group Website
[11] EHRS-Blueprint (v2) (Full) | Canada Health Infoway (infoway-inforoute.ca)
[12] OpenHIE Architecture Specification - OpenHIE (ohie.org)
[13] National Digital Health Blueprint Report for Public
[14] Comments | Ministry of Health and Family Welfare | GOI (mohfw.gov.in)
[15] Digital health platform handbook: building a digital information infrastructure (infostructure)for health (who.int)

2.4.1 Digital Health Blueprint

The primary objective of the digital health blueprint (referred in this document as "the Blueprint") is to establish a shared understanding and vision of an interoperable digital health record in the country of Sri Lanka. In keeping with the discipline of enterprise architecture, this document presents a series of perspectives of an envisioned future state of the digital health system in Sri Lanka.

A digital health blueprint is analogous to a blueprint for a building, in that it defines the overall shape and requirements of the building (number of rooms, layout, etc.). However, for implementation/ construction of the building to progress, further detail must be expressed for electrical wiring, plumbing, heating, and cooling, etc. The SL-DHBP follows this pattern through its architectural views (see section 2.3 on page 25).

2.4.2 National Electronic Health Record (NEHR)

In this document, a national electronic health record is used to describe the collection of health information captured about a citizen through various care providers connected to Sri Lanka's digital health platform. A client's NEHR is populated as the client seeks and is provided care through the numerous services connected to the health enterprise in Sri Lanka.

The ultimate goals of the establishment of a digital health record for citizens in Sri Lanka is to facilitate lifelong care of the client across digital health solutions. The requirements of which are described in section 3.2 (on page 47).

2.4.3 Digital Health Service (DHS)

In this document the term digital health service is used to describe an enterprise service with a particular area of concern and function. This service should encapsulate all the business processes, technology, and interconnectivity to provide one or more business functions related to a particular function within a business domain.

2.4.4 Digital Health Platform (DHP)

In this document, a digital health platform is used to describe the people (medical officers, government officers, support, and administrative staff, etc.), organisations (ministries, NGOs, private sector institutions, etc.), places (clinics, hospitals, etc.), business processes, technologies, and standards that facilitate the interchange of a client's NEHR between stakeholders. This includes core and support services such as:

- Mechanisms for uniquely identifying people, places, services, providers, organisations, and events.
- A patient-centred digital health record for every citizen of Sri Lanka.
- Mechanisms to facilitate the delivery of care including decision support, workflow and case management, and cross-vertical care.
- Services to support centralised public health monitoring, research, and financial and resource planning.
- Mechanisms to protect and monitor a client's privacy.
- Infrastructure built on existing Sri Lanka government resources (Lanka Government Cloud, Lanka Government Network, National Data Exchange Services, etc., and to be expanded with private sector resources) to ensure reliable, secure, and highly available communications.

The DHP encompasses the health information exchange of Sri Lanka and all related technical and business services, policies, secondary use, and supporting personnel.

2.4.5 Point of Service (PoS)

A point of service application is used to describe any environment (clinic, hospital, community health app, etc.) where clients seek, or receive care from providers. These systems typically are specialised and operated by various government, provincial council and private sector institutes.

Examples include:

- HHIMS – Hospital Health Information Management System
- HIMS – Hospital Information Management System (and SWASTHA)
- Cloud HIMS
- eRHMIS for reproductive public health
- LeMIS – Leprosy Management Information System
- eIMMR – electronic Indoor Morbidity and Mortality Register

An assessment of digital health interventions found in Sri Lanka can be found in the HIS Evaluation 2019 (referenced document #4).

2.4.6 Digital Health Information Warehouse (DHIW)

The digital health information warehouse provides summary information about population health of organisational units within Sri Lanka (such as provinces, regions, or private care settings). The warehouse is the basis upon which reporting, financial and capacity planning activities, and public health decisions can be undertaken by the MOH.

The DHIW is also commonly named the Health Management Information Services (HMIS). Because the terms HMIS, HIMS (Hospital Information Management System), and HHIMS (Hospital Health Information Management System) can easily be confused, the term DHIW and "secondary use" are used in this document in lieu of HMIS.

The digital health information warehouse defines and subsequently collects key performance indicators (KPIs) either:

Directly from point of service (PoS) applications (i.e., data that is reported in aggregate directly by the point of service application).

By querying digital health services in the DHP to compute aggregates (or asking those services to produce reports) on a particular reporting cadence.

By monitoring events in the DHP and computing aggregates in near real-time manner.

The physical realization of the logical DHIW component services within the DHP are not specified in this document and will support a variety of use cases and data within many contexts. The term DHIW is used to encapsulate all secondary use and reporting mechanisms within the DHP. Technologies which envisioned to service the role of DHIW are:

- Traditional Data Warehouse & Data Mart services provided by relational databases (using ETL or ELT)
- Data Lake and Data Mining services
- Online Analytical Processing (OLAP) Cubes
- Specialized health management information services provided by District Health Information System (DHIS2), or the current eIMMR solutions.

2.4.7 Record Locator / Index

In this document, the term record locator (or index) is used to describe a service which provide pointers to patient information across data repositories. Authenticated parties with the correct authorization level may search the index to locate data within domain repositories, registries, etc. which may represent a common client, event, etc.

For example, querying a record index for all data related to Sanduni Perara may yield blood test results in a lab repository, a discharge summary in the NEHR repository, a diagnostic image in a hospital system, and more.

Indexes contain metadata about the information stored in repositories. An index primarily stores only minimal metadata information required to fulfil queries and a pointer to where the data resides in the DHP. An aggregator will then use these results to obtain the details of this data from the relevant repository of information.

2.4.8 Repository

A domain repository is used in this document to describe a digital health service which stores, disseminates, and protects clinical data which makes up a component of the client's NEHR. Repositories can store preliminary data, unconfirmed data, data which is negated (for negative results), and summaries (like discharge notes, referral notes, or visit notes).

Repositories can be monolithic in nature (where only one repository exists for all clinical information), but should be federated (between provinces, districts, or jurisdictions), delineated across disease specific vectors (such as Non-Communicable Diseases, HIV/AIDS, diabetes, or immunisation). Additionally, specialised points of service providing detailed tests, studies and procedures (such as a PACS or RIS in a hospital system, lab system, a digital pathology lab, etc.) can also be considered repositories of information in the blueprint if they expose data in standardised forms.

2.4.8.1 Registries

In the context of the blueprint, the term registry is used to denote a digital health service which provides authoritative/official records which are referenced within the DHP. Whereas a repository makes no supposition of the "official" status of data, a registry's primary goals is to establish an official (or golden) record for data.

2.5 Guiding Principles

This section describes the architectural principles which form the foundation of the Blueprint, the DHP, and the digital health solutions contained therein. A principle is a fundamental truth or proposition that serves as a foundation for a system of beliefs. Principles should be used to guide strategic planning, prioritisation, and design decisions. Solutions that align to these principles offer a basic level of compliance to the Blueprint architecture.

All partners involved, including vendors, care delivery organisations, NGOs, and MOH staff should strive to align with these principles in any business processes, procurements, development activities, software systems specifications, and policy development activities undertaken.

2.5.1 Patient Centred

The digital health platform described in the Blueprint is intended to store and provide access to information primarily for the purpose of providing health services for the benefit of patients. The DHP and its transactions, events, and services will be designed with the citizen/patient centric pattern in mind (for example, as opposed to case-centric design), with the goal of providing the right information to the right person at the right time along the entire continuum of care wherever possible. Solution designers will strive to develop citizen-first, citizen-focused solutions to benefit all citizens of Sri Lanka.

2.5.2 Aligned to Values

Stakeholders will collaborate to design systems that will strive to uphold the national values of Sri Lanka. Particularly, that of universal health coverage, free access to healthcare, the right to health, universal equity, and justice.

Recognising patients do not all start from the same place, adjustments should be made to processes, designs, and policies to correct imbalances with the goal of inclusiveness and leaving no one behind. Systems will be used for the education and empowerment of citizens and healthcare workers where possible. Intentional and unintentional barriers arising from bias or systemic structures should be identified and reasonable attempts made to eliminate them.

2.5.3 Culture of Information Sharing

The enterprise architecture blueprint for Sri Lanka seeks to broaden access to clinical and administrative information across agencies between patients, clinicians, health administrators, researchers, and other stakeholders. Solutions should support the sharing of accurate, timely and relevant information to support the administration and delivery of care and foster appropriate and transparent access to patient information with all system stakeholders.

The digital health blueprint will encourage all participant systems to provide appropriate access to information that is suitable to be shared. As relevant health events occur, details will be shared with the national digital health infrastructure.

Events should be captured with discrete, machine-readable data wherever possible (patient, provider, location, substance, event, etc.) to maximise the possibility for machine-processable re-use but should also be communicated in a context-specific package to provide additional clarity about the specific care situation. The infostructure[16] will consolidate and assemble views of data rather than through periodic extracts to provide dynamic reporting through dashboards that will always remain current.

Participant systems in the solution should allow consumption of data from their repositories where practical. Patient information will be housed in a decentralised manner, with source systems sharing only information that is suitable to be shared. Information from source systems will not be routinely replicated.

The Blueprint shall be comprehensive and inclusive in covering all relevant areas of healthcare workflow and information exchange across domains and jurisdictional boundaries to provide a complete national solution.

2.5.4 Value for Providers and Government Officers

The digital health infostructure must be designed with a focus on creating value in each service, transaction or functionality that is created for individual or institutional providers of care (such as delivery organisations, central and provincial ministries of health, and health workers). The infostructure must always seek to provide benefits to providers and avoid obstructing workflows, duplicating work, or introducing complexity. Solution designs should be created directly with the end-user where possible, and solutions must treat provider user experience as a top priority.

Benefits such as reduced data-entry burden, seamless information flow, common authentication processes, and clinical decision support will help to enable organic adoption by providers of care. The DHP the Blueprint describes will enable data-driven and evidence-informed decision making. The health information related resources stored and shared using the platform will be trusted, reliable and of high quality, and therefore will be suitable for use directly in patient care for evidence-based decision making, care accountability measurement, executing computable care guidelines and for the accurate reporting of outcomes through KPIs and data elements.

[16] "the DHP ties applications together through a standards-based, information infrastructure, called the 'infostructure', that consists of an integrated set of common and reusable components" - https://apps.who.int/iris/bitstream/handle/10665/337449/9789240013728-eng.pdf pg. vii

2.5.5 Security and Privacy by Design

By design, digital health solutions implemented in Sri Lanka will secure sensitive patient and administrative information from unauthorised access to protect privacy. Security and privacy analysis will be conducted as a first order activity during solution design, and not as an afterthought during implementation.

In providing broader access to sensitive information, the custodians of clinical data (hospitals, ICTA, the Ministry of Health, or organisations which store clinical information) must develop processes to manage security breaches, data compromises, and the scope/impact of such breaches.

Solutions and technical architectures of health systems deployed in Sri Lanka should include appropriate analysis and documentation of risks, contingencies, and validation that unauthorised access is prevented (where possible) and documented/identified. Stakeholders which are custodians of health information (clinical, or administrative) must establish protection strategies and policies within their organisation which align with the blueprint.

The security of private health information in transit and at rest is of utmost importance. The auditing of access and reporting of security breaches in a timely manner ensures that appropriate mitigations and corrective actions can be taken in a timely manner.

The analysis and documentation of risks associated with digital health solutions prior to integration with the national health infostructure will provide an understanding of what personal health information (PHI) is being collected and for what purpose, how PHI may potentially be leaked or disclosed, and allow for informed implementation of risk mitigations.

All artefacts, architectures, integration guides, etc. must include a security considerations section. Solution and domain specifications must include implementation guidance regarding minimum security constraints and contents of audit events.

2.5.6 Blueprint is Authoritative

The Blueprint is the authoritative reference for integrations within the health enterprise of Sri Lanka at national, provincial, programme, and health institution levels. Disagreements between system designs and patterns of integrations will arise as systems are integrated, but it is important to identify and maintain an authoritative design pattern.

All health IT activities undertaken by stakeholders (such as central and provincial ministries of health, private and public healthcare institutions, and vendors) must, where possible, align to the Blueprint. Classification of assets within the common framework helps with assessment of solution applicability and a common language used to describe systems. Providing common assessment tools for vendors and developers to understand how they fit within the broader enterprise.

The structure of regional, provincial, and national IT architecture documentation, plans, and assets should follow fundamental structures set forth by the Blueprint. Establishing a consistent level of requirements for solutions documentation will allow for faster assessment of solutions prior to integration. Solutions and integrations must adhere to the Blueprint, and in the case of a fundamental disagreement, either the Blueprint must be updated to reflect the new approach (and all other system designs using this pattern are updated), or the integration approach or solution must be redesigned.

2.5.7 Vehicle for Cost Effective & Efficient Investment

The Blueprint will aid as a vehicle to guide and support investment in digital health solutions in Sri Lanka. The Blueprint seeks to support the investment decisions of the central and regional agencies operating within Sri Lanka to ensure alignment to the core principles of the digital health enterprise. Investment decisions should be made in solutions that are architecturally aligned to the Blueprint, while supporting the strategic goals of the broader health system. To reduce waste and promote the organised rollout of an integrated health system, it is critical that future investments align with the vision and roadmap of the Blueprint. Sri Lankan authorities will include alignment to the Blueprint as a requirement for planning and procurements in future projects.

The architecture must be defined to maximise benefit to providers while minimising costs of implementation and operations for project sponsors, care providers, and government agencies. Designs must find a balance of sufficient quality and being suitable for purpose, while also being simple and minimalistic, scalable to national levels and provide a cost-effective model that allows complexity to be absorbed and deployed in an iterative fashion. Investments will strive to maximise utilisation of available resources and be built for sustainability. Investment decisions will involve suitable governance and transparency. Solution designs will be able to sustain growth across geographical expansion, the expansion in the number of users and the increased integration of legacy systems.

2.5.8 Leverage Existing Assets

The Blueprint will consider the ecosystem of practices and solutions that are currently operated in Sri Lanka and will identify how these existing assets fit into the conceptual constructs of the architecture defined. Duplication of business functions within the broader e-health ecosystem is inefficient and should be avoided.

Existing investments in systems will survive and prosper through the development of supported integration strategies. Solution documentation should articulate the business services and uses of each shared service in the infostructure so that ecosystem partners can clearly identify the function of shared assets and plan for integration.

Future developments of digital solutions should, where feasible, algin and leverage the existing services provided via the DHP described within the Blueprint. In cases where shared services are not feasible, attempts should be made to address gaps with existing solutions, rather than recreation of functions.

2.5.9 Encourage Innovation, Competition and Partnership

The digital health ecosystem should be open and available to all suitable stakeholders, citizens, vendors, and healthcare providers within Sri Lanka, allowing for individuals to innovate and expand the existing constructs, participate in the creation of innovative technology, and compete with one another on a level playing field.

Design decisions should include all appropriate stakeholders. Public/private engagement is encouraged where possible with the goal to provide better care for all. Technical documentation should be openly available for vendors and innovators. Open standards should be transparently developed and disseminated to stakeholders.

2.5.10 Evolutionary Development

The Blueprint will expand as new features and technologies become available. The enterprise architecture described in the Blueprint are the core health information services the country will rely on. The requirements and technologies available to support these services continually change over time, however resourcing to re-create or re-envision services is limited.

The Blueprint will strive to ensure that architectural decisions made within domains facilitate functional growth of the infostructure while maintaining the operation of existing functions through both incremental and transformational change.

For example, new platform features can be added while maintaining backwards compatibility with existing applications. This seeks to reduce the rigidity and change management burden of the enterprise and increases adaptability. The architecture will support incremental development, allowing for near term results and rapid return on investment.

2.5.11 Standardisation of Process and Services

Services and business processes related to data and information management, specifically in relation to the interaction of stakeholders with the DHP, should be aligned wherever possible.

The DHP described by the Blueprint will be designed using mature enterprise computing and service-oriented architecture approaches, ensuring that interactions with the digital health platform are stable, persistent, and dependable. Consistent processes between organisations increases data reliability and consistency.

All digital health solutions should provide business use cases of their interactions with the information exchange. Design specifications should also consider availability, scalability, reliability, and maintainability. Solutions must also be performant, scalable, and measurable.

2.6 Uses and Benefits

This section is intended to assist in setting the context for the Blueprint. Developing a blueprint is a critical step towards enabling standardisation and interoperability between siloed health systems across a jurisdiction. The Blueprint enhances and accelerates the development of digital health services and applications within the national digital health strategy. It also aids to align stakeholders and to achieve consensus, creating an efficient path forward to achieve national healthcare goals.

The following sections provide an overview of the potential uses and benefits of an architecture blueprint, and how they apply to the various individuals, organisations and stakeholders that interact with the national digital health system in the future. One of the primary purposes of the Blueprint is to act as a frame of reference and set of common definitions and principles for the teams that are working on health information sharing initiatives across the country.

The Blueprint has been developed based on the needs and requirements collected from the various stakeholders that are operating clinical and health information system operations in Sri Lanka, as well as the experiences gained from initiatives in other countries around the world.

2.6.1 Uses of the Blueprint

The following sections describe the potential uses of the Blueprint and the DHP it describes.

2.6.1.1 Framework of Reference for Strategic Planning

The healthcare sector of a nation is comprised of many stakeholders and systems. The Blueprint assists in providing an overall view of the national digital health system will be realised and enables stakeholders and project teams to align their systems so that they can to be incorporated in the future. The Blueprint will serve as a valuable strategic input document that can assist officials in their decision making, planning and investment in digital health solutions.

2.6.1.2 Tool for Promoting Country-wide Standardisation

The Blueprint promotes a common understanding of the future state of health information sharing in Sri Lanka. Operating within this context allows projects across the country to coordinate and align their work within this common framework and achieve interoperability.

The use of a blueprint establishes key terminology for communicating between stakeholders with various backgrounds. Stakeholders will be better able to identify and describe their requirements and be better able to understand potential solutions as they are presented.

2.6.1.3 Guiding Conceptual Designs of Specific Implementations

The Blueprint provides a conceptual architecture of the national digital health platform (DHP) for Sri Lanka. This accelerates the architecture phases of individual projects by reducing effort and provides valuable input into the design and development phases. The Blueprint can also be used as a supporting document in the early phases of project initiation, to set context, help acquire support from stakeholders or funding from project sponsors.

2.6.1.4 Investment Evaluation

The Blueprint will become a key asset used during project initiation phases to assist in setting context for programs or projects. Evaluation criteria could be established that assess the conformance of the proposed program or project to the Blueprint and this information could be used to guide investment.

2.6.1.5 Framework for Education, Training & Skills Development

The Blueprint provides a framework for education, skills training and capacity development in digital health solutions. Common nomenclatures and concepts should be introduced into the various skills development programs across the country. This will aid in the transition to a digital health environment.

2.6.2 Benefits of the Architecture Blueprint

The following sections describe the primary benefits of the Blueprint categorised by conceptual stakeholder group.

2.6.2.1 Benefits for Patients & Advocates

Providing a national blueprint for digital health allows patients, their advocates and supporting organisations (for example, Sri Lanka Association for Child Development) in the understanding of the future digital health infostructure. In doing so, innovative applications that make use of the services in the infostructure can be further developed, allowing patients ownership over their own clinical records in specialised tools customised to their condition. This includes use cases such as digital proof of procedures, prophylaxis, immunisation records etc.

2.6.2.2 Benefits for the Line Ministry and Provincial Ministries of Health

Developing a blueprint is a critical step towards enabling standardisation and interoperability between siloed health systems and across the various programmes delivered by the Line Ministry and Provincial Ministries of Health in Sri Lanka. The architecture manifests a national digital health vision and mission into a tangible framework for deploying digital health services. Use of a common blueprint accelerates the development of digital health services and applications within the national digital health strategy, and provides guidance that can be leveraged throughout provincial and regional directorates of health.

The Blueprint will also be used as a tool to achieve stakeholder consensus on national strategies and priorities. The blueprint can be used as a framework for classifying initiatives to make the most effective use of limited resources and funding.

Finally, a common blueprint assists in guiding national digital health investments. This allows for capital and donor based activities to be aligned, reducing of duplicated efforts and prioritizing strategic digital health interventions. The alignment of all the in-country digital health initiatives provides clarity to donors and implementer in regards to the services, requirements, roles, responsibilities and governance of the digital health innovations in Sri Lanka.

2.6.2.3 Benefits for Technology Innovators, Software Development Organisations and Vendors

Establishing a blueprint benefits Sri Lanka by increasing the agility of health technology innovation. The Blueprint provides clarity and direction to innovators, software development organisations and solution vendors, lowering their costs, timelines, and risks of systems development and/or procurement.

The Blueprint achieves this is by simplifying and standardising information exchange protocols within the health sector of the nation. Using a platform approach also accelerates and simplifies software development and future enhancements by re-using common platform components across health domains and jurisdictions.

With this platform in place, client applications can leverage complex business processes and datasets available in the infostructure to achieve business objectives. For example, the Blueprint architecture will allow innovators to develop specialised "apps" to make use of information gathered by other digital health software applications without the need for point-to-point integration between (or even knowledge of) those other applications.

Information standardisation specified in the Blueprint and the companion artefacts such as the Interoperability Plan ensures that applications work with data that is consistent, understandable, accessible to, comparable to, and compatible with other applications across national digital health programs and services. Using consistent interoperability specifications across the nation allows for innovation and diversity to occur in local and provincial systems, but also ensures compatibility with a known national infostructure.

The consistent use of nomenclature in solutions also improves understanding and communications within care teams and across organisations, and ultimately improves accuracy in national reporting and allows technology developers to better understand where their solution fits within the broader national digital health infrastructure.

2.6.2.4 Benefits for Healthcare Institutions

Healthcare institutions benefit from having a national blueprint. Hospitals, private clinics, agencies, and non-governmental organisations can use the Blueprint to assist in solution planning for their individual goals and needs. While these entities will all be at very different stages of technology adoption, the Blueprint can be used as a support tool during strategic planning exercises for digital transformation.

The Blueprint and the digital health platform it proposes directly assists healthcare institutions via the information sharing ecosystem is establishes. The sharing of clinical data allows institutions to reduce costs by preventing the duplication of clinical investigations, reducing data entry errors, duplicate data entry, and consistent identification of subjects of care and materials at the point of care.

The Blueprint also presents an opportunity to drive change management and knowledge transfer. This will aid in the adoption of common digital processes used by healthcare professionals, and support staff.

2.6.2.5 Benefits for Clinicians and Healthcare Providers

Publishing the Blueprint provides a common framework and set of consistent nomenclature to assist in meaningful collaboration between colleagues across the health and ICT domains in a secure manner. This allows providers to securely access data and influence the direction and prioritisation of investments in digital health technologies.

The DHP that the Blueprint describes also allows providers to use shared infrastructure to portably apply their skills (i.e., after transfer, private practice, telemedicine, or remote medical services). Streamlined access credentials reduce the burden of remembering multiple logins, changing passwords, or updating contact information.

Healthcare providers can also use the blueprint to participate and influence the development and implementation of the national digital health infostructure to achieve the broader goals of quality care processes such as known, consistent procedures for data capture and faster dissemination of health event information to and from other facilities.

Understanding the architecture allows providers to monitor and evaluate digital health implementations and interventions as they are developed. By utilising consistently applied terminologies and workflows described in the blueprint, the health workforce becomes more efficient by having the ability to port their knowledge and skills between organisations across the country.

2.6.2.6 Benefits for Health Professional Councils

Health professional councils such Sri Lanka Medical Council and Sri Lanka Nursing Council and other bodies can use the blueprint to envision future state policies and workflows related to national information presentation and sharing, member education, and the performance and measurement of patient outcomes.

The Blueprint will also assist in envisioning how the infostructure can be used to improve patient outcomes through utilising clinical decision support and/or expert systems. Associations can also use the blueprint to help guide policy creation for data collection and research use of data.

2.7 Key Assumptions, Decisions and Limitations

This section defines the key architectural assumptions and decisions made during the development of the Blueprint.

The assumptions made in the development of the Blueprint were:

i. The SL-UDI (Unique Digital Identity) platform will be available and will provide compatible interfaces (using OAUTH and/or OpenID) made available for the health sector for the DHP.

ii. Any supporting security (one-time passwords, password complexity, access control), human resourcing (enrolment and deactivation of users, transfer, and assignment of providers), and technical policies and procedures will be developed independent of the blueprint by relevant agencies in Sri Lanka (the NDHGS [2] document contains guidelines for these).

iii. Public and private health care institutions have reliable connectivity (e.g., hard-wired fibre optic internet) and can accept requests to service queries from known consumers.

iv. There is an acceptance to use health care standards and a willingness among implementers to implement them.

v. The maintenance of independent data producers to be directly queried by other connected systems on the DHP would present a significant level of effort for operators, network, and software developers as each revision to the standard document would require software updates to each connected system.

vi. Implementers of digital health services which participate in the DHP will understand the National Digital Health Guidelines and Standards [2] document including the onus of their organisation whenever operating or developing software for Sri Lanka.

vii. Operators of digital health services (custodians of data) will be responsible for the maintenance and implementation of their own policies which protect patient privacy, security of IT systems, etc.

viii. Blueprint version 1.0 is meant to provide an extensive description and presentation of a potential future state (10 – 20-year horizon), this framework and blueprint will evolve through stakeholder engagements to develop future revisions 1.1, 1.2, 1.3, etc.

ix. The Sri Lanka digital health Blueprint version 1.0 was developed using an agile methodology led by the Sri Lanka Ministry of Health, along with various national stakeholders and national and international technical assistance during the summer of 2022. Ongoing travel and meeting restrictions required that much of the work for version 1.0 be conducted remotely. This was effective at establishing an initial first version; however, it was not ideal from a collaboration standpoint, and may have introduced gaps such as missing or incomplete stakeholder feedback and assessments. It is expected that the Blueprint will continue to evolve beyond version 1.0 with intensive feedback from additional stakeholders, and subsequent versions will be released later.

2.8 Evolution of the Blueprint

Under the mandate of the NeHSC established in 2019, a technical working group was appointed for the development of the National Digital Health Blueprint and Health Information Exchange (TWG-BluePHIE). In the process of developing a blueprint, the TWG-BluePHIE observed a deficit of an overarching National Digital Health Strategy that would align the scope of the blueprint with the national digital health vision and mission. Because of this, the document scope of the original blueprint expanded from a National Digital Health Blueprint to a National Digital Health Enterprise Architecture plan. This plan set the framework for the capture of requirements, provided an initial series of analysis, and an initial series of needs assessments with relevant stakeholders.

2.8.1 Identification of Key Stakeholder Groups

From the outset, digital health capabilities and services defined in the Digital Health Blueprint have been based directly on the needs of key stakeholders. During the development of the DHEAP mentioned above, an exhaustive list of stakeholders was identified and prioritised, and these groups have been consulted from the beginning of the development of the DHEAP and the Blueprint. Live in-person workshops were conducted where needs were identified and documented, and capabilities and services were identified to satisfy those needs. Ongoing assessment meetings of the status of the digital health interventions being used by various programs are being conducted during the development of the Blueprint to ensure alignment to needs.

Key stakeholders include relevant DDGs, public health programs in operation such as the National Cancer Control Program (NCCP), Non-Communicable Disease Unit, Deputy Director Generals (DDG), Health Information Unit (HIU), Family Health Bureau, ICTA and more, as well as operators of existing curative and preventative sector health information systems across the country such as the Hospital Health Information Management Systems (HHIMS), Hospital Information Management System (HIMS) SWASTHA.

2.8.2 Landscape Assessment and Business Context

To set realistic and achievable targets for the national digital health program, the working group conducted a detailed landscape assessment evaluation of current health information systems active in Sri Lanka using the MAPS framework[17].

[17] Evaluation of Electronic Health Information Systems (HIS) [5] https://arch-lk.health/dmsf/files/3/view

To gain a thorough insight into the business context of digital health in Sri Lanka, the DHEAP reviewed several National documents and publications, including:

- Annual Health Bulletin – for insights on population health, health system status and challenges
- National Health Policy – for insights on the vision, mission, and health policy goals of the country
- National Health Strategy Master Plan 2016-2025 – for identification of health strategic priorities
- The Annual Report of the Central Bank of Sri Lanka for insights on the economic and social development goals of Sri Lanka
- Health Information Policy of 2017 – insights on guiding principles and main strategic areas pertaining to Health Information

2.8.3 Establishing Digital Health Needs

One of the most important steps of the DHEAP development process was to identify, collate and discuss key stakeholders who would benefit from digital health interventions. MOH carried out a workshop in 2019 to sensitise the field level stakeholders and identify their digital health needs.

The primary workshop process had three distinct sessions:

- Sensitisation and knowledge sharing sessions
- Digital Health needs identification sessions and mapping
- Discussion sessions between organisations

2.8.4 Creation of the Digital Health Blueprint Artefacts

After the development of the DHEAP zero draft, the development of a comprehensive framework for digital health enterprise architecture (and health information exchange) was undertaken, using an agile sprint development methodology. The HI & HQ project has been supporting this piece of work since July 2021.

MOH and ICTA with technical assistance provided by international consultants (ITA) and national technical consultants (NTA) engaged in a collaborative authoring process to co-develop a framework for a holistic approach for digital health integration.

This initiative resulted in the creation of key enterprise, conceptual artefacts including:

- Digital Health Blueprint
- Interoperability Plan
- Interoperability Profiles
- Sustainability and Resourcing Plan
- Procurement Plans

This set of documents will serve as the basis for implementation and realization of the blueprint.

2.9 Stakeholder Engagement

The MOH will continue to engage with stakeholder groups identified within the DHEAP document throughout the development of the Blueprint using the process illustrated in Figure 4. To optimise the feedback from stakeholders, version 1.0 assets of the digital health enterprise architecture will be presented, and feedback iterated into the draft to ensure that each of the assets developed in the enterprise architecture meet the expectations and needs of stakeholders (which were previously captured during the landscape assessment phase of the DHEAP development). Subsequent releases will be made available, disseminated, and iterated until validation has been achieved.

Throughout the process documents are edited and uploaded to the Sri Lanka Digital Health Architecture Blueprint Redmine site, a collaborative platform that allows for dissemination of tasks, documents and other assets between relevant authors and stakeholders.

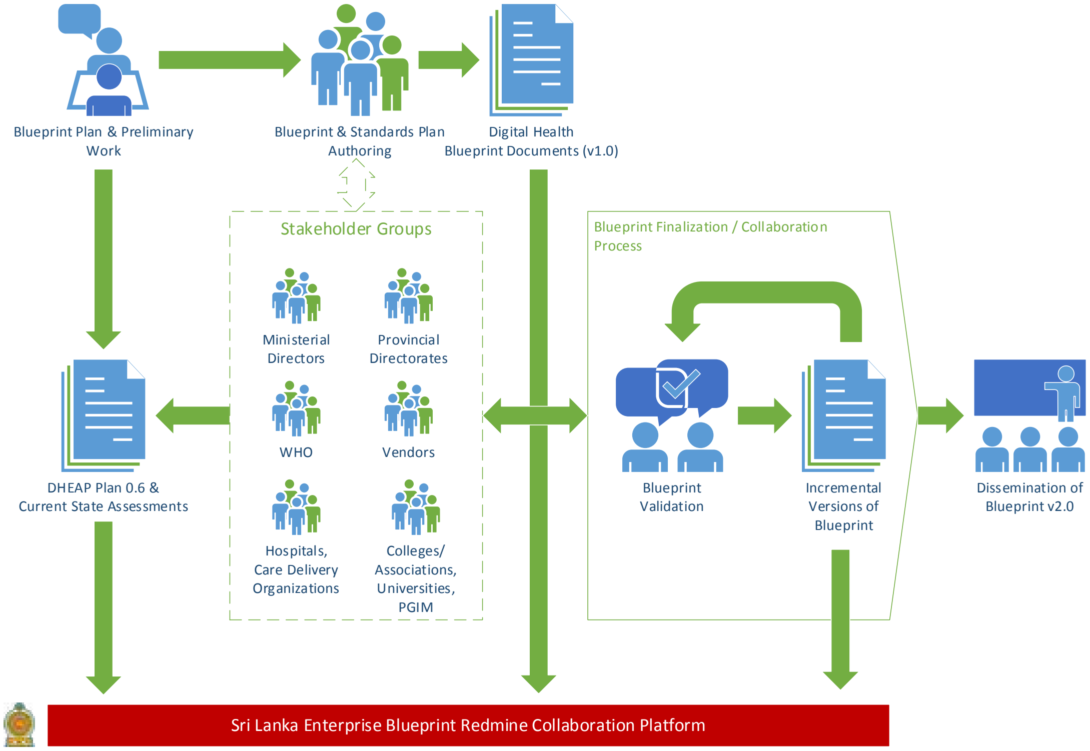

Blueprint Plan & Preliminary Work
Blueprint & Standards Plan Authoring
Digital Health Blueprint Documents (v1.0)
Stakeholder Groups
Ministerial Directors
Provincial Directorates
WHO
Vendors
Hospitals, Care Delivery Organizations
Colleges/ Associations, Universities, PGIM
DHEAP Plan 0.6 & Current State Assessments
Blueprint Finalization / Collaboration Process
Blueprint Validation
Incremental Versions of Blueprint
Dissemination of Blueprint v2.0
Sri Lanka Enterprise Blueprint Redmine Collaboration Platform

Figure 4 : *Stakeholder Engagement Plan*

The stakeholder groups identified in the DHEAP include:

- Ministerial Directors: Curative (DDG MSI, DDG, MSII, DDG Lab), preventative (DDG PHSI, DDG PHAS II), Logistics (DDG MSD, DDG Bio Medical and HR)
- International Agencies: The World Health Organisation, World bank, Asian Development Bank, and UNICEF
- Provincial and Regional Directorates
- Colleges/Associations, Universities and PGIM
- Care Delivery Organisations: Primary Care Units, Government and Private Sector Hospitals (Teaching, District and General)
- Institutes contributing to streamlining digital health services, including: ICTASL (PVT) LTD, SL-CERT(PVT) LTD, TRCSL, HISSL, SLCHI, SLMC, NMRA, SLNC
- Patient Groups
- Trade Unions
- Vendors: Telecom Providers, Network Companies, and Hardware Vendors

3. Business Architecture

3.1 Current State

The current state business architecture of the Sri Lanka Health Enterprise has been adapted from the DHEAP [1] document and illustrated in Figure 5.

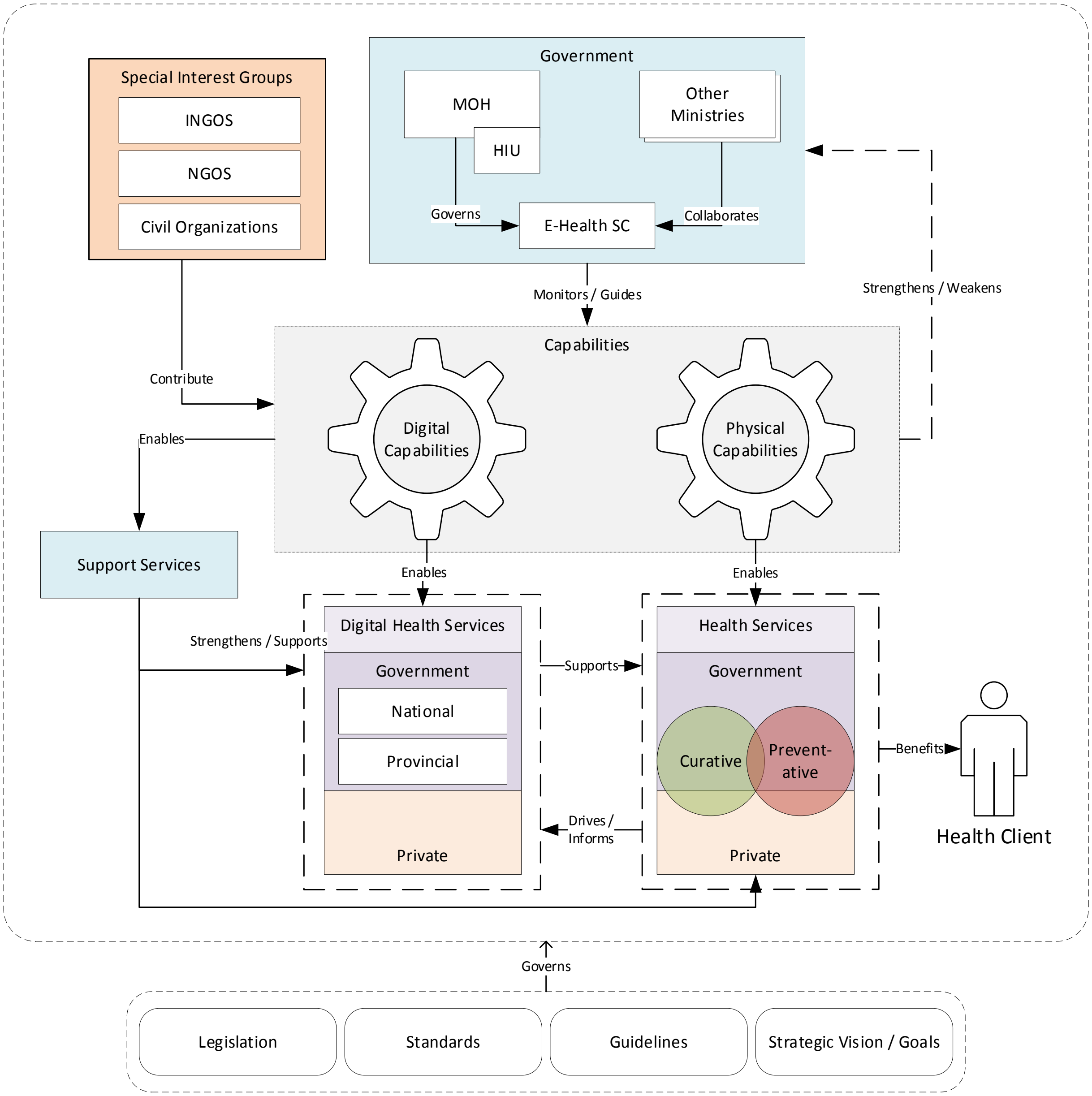


Figure 5 : *Current Enterprise Business Architecture*

The Ministry of Health is the governing body which is primarily responsible for the E-Health Steering Committee (EHSC). The steering committee with the assistance of other ministries (such as ICTA) and under the guidance of the Health Information Unit (HIU), as the national focal point will monitor and guide the capabilities of the health sector:

- Digital Capabilities: The use of health information systems for care delivery, management, reporting, monitoring and protection of data used for the delivery of care. This includes the technology resources, software packages, and supporting infrastructure.
- Physical Capabilities: The personnel (nurses, doctors, administrators, and other health workers) and physical infrastructure (such hospitals and clinics) which are used to deliver care to patients via health services offered in Sri Lanka.

The current and future physical (new devices, clinics) and digital (DHP, registries, etc.) capabilities of the sector will, in turn, either strengthen or weaken the ability of the EHSC to realise objectives set forth by the national policy on health information[18]. Additionally, these capabilities will guide the ability of Sri Lanka to deliver and implement health services (digital and physical) provided by government bodies at the national and provincial level, as well as the private sector.

The capabilities enable supportive services for digital health services and health delivery services. These support services include human resourcing management, procurement and supplies management, policy and procedure dissemination, and other such services which strengthen digital health services. Digital health services, in turn, support the delivery of preventative and curative health services delivered by government and private institutions for the benefit of health clients.

3.1.1 Business Structure

This document provides only a summary of the MOH structure relevant to digital health and is not intended to provide an in-depth description of the organisation of the central or provincial ministries of health. A detailed organisation chart for the Sri Lankan MOH structure can be found in the Sri Lanka Health System Review produced by the Asia Pacific Observatory on Health Systems and Policies[19], which provides an in-depth view of the organisational structure of the Ministry of Health which was summarised in section 1.1 on page 18 of this document.

The Director General of Health services (DGHS) is the technical head of the Ministry and is supported by multiple Deputy Director Generals (DDGs) most of whom are specialist medical administrators or specialist community physicians. Under the DDGs are separate units headed by directors (examples: Health Promotion Bureau, Quarantine Unit, etc.). The Health Information Unit resides under the DDG Planning, and is the national focal point for health information and digital health, as mandated by the National Policy on Health Information-2017[19].

The Information Communications Technology Agency (ICTA) provides guidance on national ICT strategies, policies, plans, standards and guidelines as well as operational IT support to the MOH.

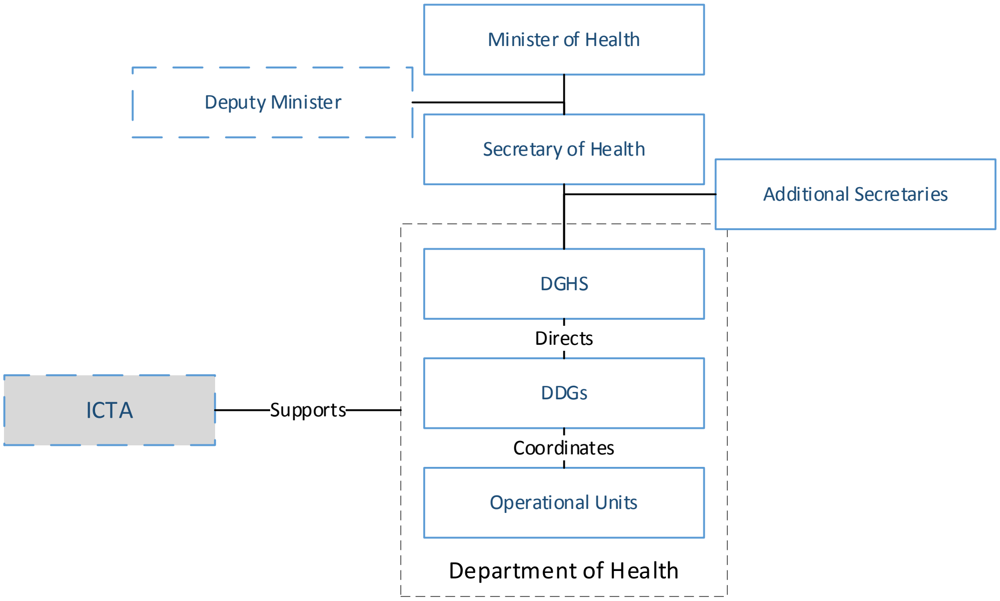
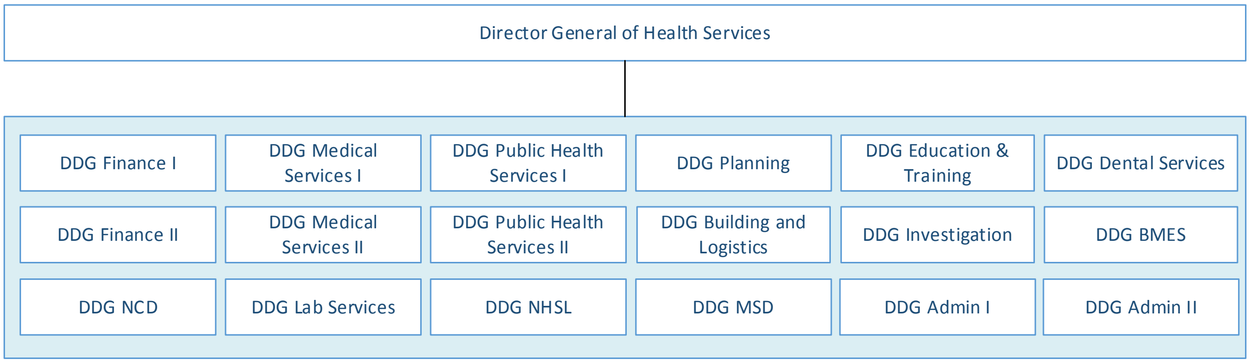


Figure 6 : *Conceptual Relation of Central MOH*

[18] PG 3569 Health Policy (E) new.indd (documents.gov.lk)
[19] *9789290228530-eng.pdf (who.int)

The DDGs are illustrated in Figure 7, and are aligned to the core operations including financing, staffing, planning, delivery, and administration of health delivery, monitoring and reporting activities. Collectively, these represent the “business users” for the Blueprint.



Director General of Health Services

DDG Finance I	DDG Medical Services I	DDG Public Health Services I	DDG Planning	DDG Education & Training	DDG Dental Services
DDG Finance II	DDG Medical Services II	DDG Public Health Services II	DDG Building and Logistics	DDG Investigation	DDG BMES
DDG NCD	DDG Lab Services	DDG NHSL	DDG MSD	DDG Admin I	DDG Admin II

Figure 7 : *Focal DDGs for the blueprint*

The primary areas of concern for each DDG at the central level is described in Annex A (page 142).

3.1.2 Provincial Health Ministries

The MOH, also referred to as the “Line Ministry”, as opposed to “Provincial Ministries”, is responsible for the primary management of health services within the country and provides stewardship for development and delivery of health services. The MOH also directly manages several large hospitals (National Hospital of Sri Lanka, teaching, and specialised hospitals, etc.) and vertical programmes and campaigns. The nine provincial health ministries are charged with the effective implementation of care within their respective provinces including primary care, secondary care, and prevention services.

The administrative head of provincial ministries of health are the provincial Secretary of Health. Provincial Directors of Health Services (PDHS) are the technical leads of each province’s health department. Each district within the province additionally has a Regional Director of Health Services (RGHS) who is responsible to the PDHS.

There are 354 Medical Officer of Health areas in Sri Lanka, each headed by a Medical Officer responsible for a defined population which, on average, is between 40,000 and 80,000 persons.

3.2 Business Drivers

This section provides insights into the business needs and drivers for the establishment of the blueprint. These drivers were attained by summarising the stated objectives of the enterprise architecture in the DHEAP (section 7) and key stakeholder engagements/current state assessments (described in more detail in Annex B on page 144) with:

- DDG Management Development and Planning Unit
- DDG Medical Services Unit I
- DDG Medical Services Unit II
- DDG PHS 1
- DDG PHS 11
- DDG Laboratory
- DDG dental services (pending)
- DDG bio medical (pending)
- DDG NCD

- DDG medical supplies
- Family health bureau
- Health Promotion Bureau
- Epidemiology unit
- Nutrition coordination unit
- Quarantine Unit
- Anti-Leprosy Campaign
- National Programme for TB and Chest Disease (NPTCCD)
- National Dengue Control Unit
- Antimalaria Campaign
- National STD and AIDS Control Programme (NSACP)

These sources were used to establish key drivers for the establishment of a national digital health platform which are described in more detail in this section:

- Address the complexity of governing digital health solutions.
- Establish a shared, patient centric, nationally scoped electronic health record (NEHR).
- Facilitate the sharing of data between digital health solutions in the private and public sector.
- Provide accurate, complete, and timely access to digital health information between stakeholders.
- Protect and secure private patient health information.
- Streamline the collection of primary care data and enable secondary uses of that data.
- Enhance operational effectiveness of the Ministry of Health through capacity building, and knowledge dissemination.
- Integrate information sharing flows between public and private care settings for delivery, prevention, referral purposes, supply and commodity management.

3.2.1 Address Complexity of Digital Health Solutions

The wide array of health services delivered within the Sri Lankan health enterprise for various purposes by different providers can lead to a challenging IT landscape from both a governance and implementation perspective.

The complexity manifests itself across many different dimensions, including:

- System Complexity: A solution supporting the wholistic delivery of care at a national or provincial level would need to support a wide range of complex domains (like Radiology, Laboratory, Pharmacy, Pathology, etc.) with wildly differing data and business process requirements and various users.
- Organisational Complexity: Health clients may seek curative or preventative care in private or government health settings in a variety of settings (hospitals, clinics, outreach, etc.).
- Human Complexity: Incorporating the use of shared health information into the day-to-day activities of providers (and, in the future, patients) requires additional training in all aspects of information sharing and use, including privacy and security, ethics, appropriateness, patient safety. These considerations must be taken by providers of care in addition to their regular clinical duties.
- Information Complexity: Storing and capturing data from different clinical domains delivered by different providers with varying systems of use increases the complexity of defining the structure and content of data including textual data, medical imaging, video, and others.
- Standardisation Complexity: Using a single standard (such as FHIR) may appear, on the surface to address the complexity of a heterogenous standards environment, however it is rare that a single standard can

be adopted for the entirety of the health domain. Several factors impact this including: appropriateness of the standard itself (DICOM WADO / QIDO is better suited for imaging, SYSLOG is faster for auditing), the capabilities and ability/cost to change existing solutions (like proprietary software solutions) should be considered when selecting appropriate standards.

- Technical Complexity: The ability to manage diverse services required for different domains, across disease vectors while providing scalable and reliable infrastructure with proper redundancy and disaster recovery procedures must be considered by any implementer of a health system.

It is often tempting to envision a single, monolithic solution to address this complexity. However, forcing a single solution into such a complex domain across specialties, use cases, and disease vectors is nearly impossible, even if such a solution is designed using microservices and REST APIs. There are simply too many disease vectors, requirements, data elements, guidelines, and users to appease to implement a one-sized solution for all use cases, making a single solution unmanageably large and inflexible to changing requirements.

For the blueprint's solution to complexity, please refer to 3.3.2 on page 60.

3.2.2 Establish a Shared, Patient Centric National Electronic Health Record (NEHR)

The primary business driver of the DHP in Sri Lanka is the establishment of a patient-centred National Electronic Health Record (NEHR). This electronic health record should be cross-cutting between connected organisations, software solutions, delivery systems, providers, organisations, and governmental bodies. NEHR will also facilitate primary healthcare reorganization currently being undertaken within the line ministry of health.

The NEHR will be accumulated from contributions driven by care events delivered from birth until death: a life-long health record.

Authorised primary and secondary use of clinical data, with the consent of the patient or mandated by law and in particular the Personal Data Protection Act 2022, should be considered a key business requirement of the DHP.

3.2.2.1 Requirements

- The DHP shall allow the storage and retrieval of discrete, identified, patient data, within legally permitted limits, for the lifetime of the patient.
- DHP shall allow the expression of consent by the patient (or the withdrawal of consent) of the use of their data for secondary use purposes such as research, planning, and monitoring.
- The DHP shall allow the computation of aggregate data on regular intervals for use for research, monitoring, ability, and planning within Sri Lanka.
- The DHP shall ease the ability to make key business decisions based on individual records where clinically or legally relevant (such as recalls of devices or drugs).
- The DHP shall provide a mechanism to allow for permanent erase of clinical data related to a patient when requested by the patient (withdrawal of consent)

3.2.3 Share Relevant Clinical Data between Organisations, Facilities and Care Settings

The DHP's primary business driver (establishing a lifelong patient centric NEHR for a patient) requires the consolidation of structured and unstructured data, documents, and notifications.

The NEHR should not be a replication of all health events from every PoS system. Rather, it should represent a curated subset of data collected from individual interactions a patient has with the health system. Clinicians often have only minutes to interact with patients, and as such, NEHR summaries should represent the essential information to provide an accurate health picture for the patient (i.e. only sufficient data for a provider to make an informed clinical decision), allowing clinicians to navigate to the source of information when required.

Examples of data which may be of use in a shared NEHR include:

- Hospitalisations and discharge summaries.
- Referrals and transfer data between points of care.
- Blood type, allergy, immunological and prophylaxis profiles.
- Communicable disease status.
- Chronic conditions and care plans related to long term care.
- Medication profiles.
- Laboratory, pathology and diagnostic imaging results.
- Organ donation and transplant recipient status.

Conversely, a client's digital health record should not include minutiae related to transactional care within a clinical setting which would provide little or no value to care delivery or secondary use. Examples of content which should not be in the shared DHP include:

- Hourly temperature, blood-pressure, and heart rate monitoring.
- Discrete data about business processes within an institution.
- Internal patient management data such as bed location, current ward, etc.

An illustration of the types of information captured at points of service and the relevant information for the national electronic health record is contained in Figure 8. The initial specification of the minimum dataset for these

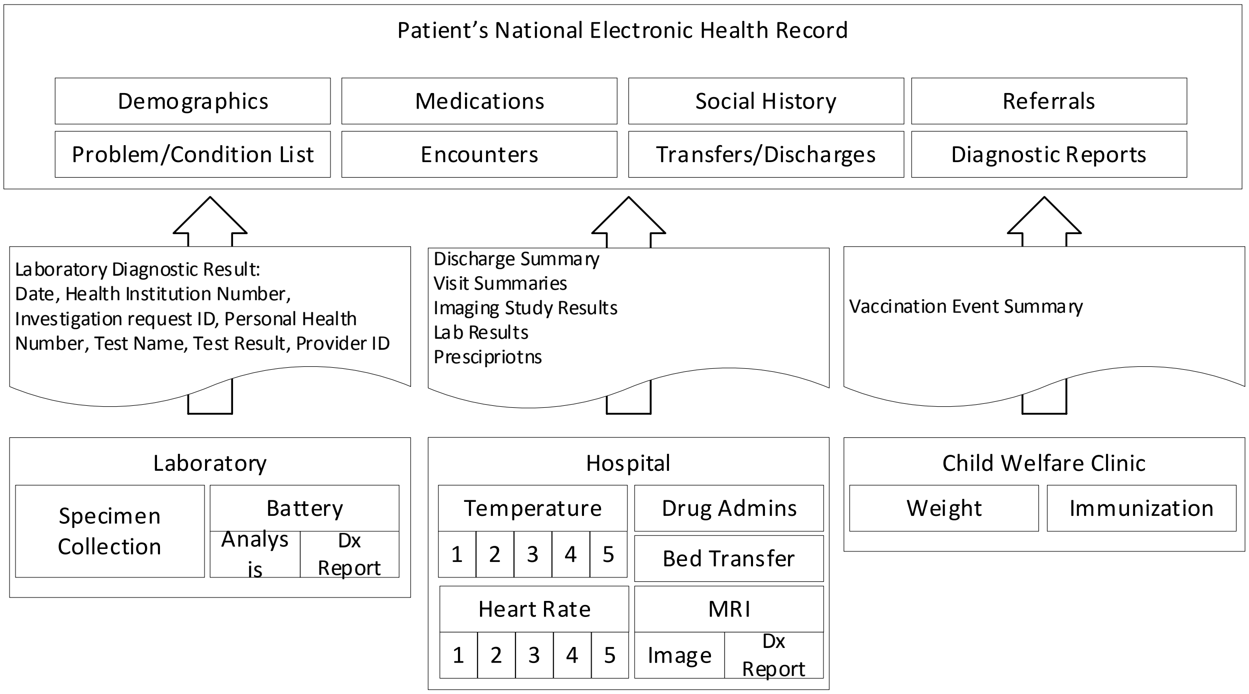


Figure 8 : *Sharing of Clinically Relevant Data*

classifications of data to be submitted to the NEHR is specified in the National Digital Health Guidelines and Standards [2] document[20].

Establishing which data elements belong in the patient's shared digital health record is a decision which must be made between stakeholders and will vary between health sub-domains. These elements are specified in each logical view so that implementers, operators, and users are aware of data which should be shared.

3.2.3.1 Requirements

- The DHP will specify in logical views, the data elements which are clinically relevant for sharing between system and organisational boundaries.
- The DHP will validate that submitted data to a patient's NEHR is valid and meets the criteria and minimum useful data elements based on the triggering event.
- The DHP shall specify in its logical views, the clinically relevant events which should trigger sharing of data with the shared infrastructure.

3.2.4 Provide Accurate, Complete and Timely Delivery of Care

Patients within Sri Lanka can seek curative and preventative care within the public or private health systems. During treatment, patients interact with a variety of solutions including hospital information systems (HMIS, HHIMS, SWASTHA, OpenMRS, CloudHIMS etc.), disease specific solutions (DenSys, eMIS, LeMIS, etc.) as well as private solutions.

To facilitate the best health outcomes for these patients, the DHP must supply to health providers using these systems with accurate and up-to-date information. This includes facilities within the DHP which allow for the querying of events which have occurred, or are intended to occur (i.e., referrals, transfers, appointments), and proposals for care (i.e., CDSS proposals).

3.2.4.1 Accurate

Whenever clinical decisions are made based on data from outside of an organisation, it is important that the provenance of that data (its origin, including surrounding context) as well as accuracy of the data is conveyed. The DHP should indicate methods of digitally signing clinical data from source, ensuring that providers consuming this information can be assured that the information is accurate, and has been reviewed. Additionally, the unaltered from of the originally submitted data should be available for clinically sensitive information. User interface techniques should also be used to report provenance to the end user of the data in question[21].

In the case where data is generated, aggregated, or translated within a DHP service, it must also be clearly identified as such. The distinction between generated, aggregated, or translated data and data which was reviewed and signed by the source provider is important, as it impacts the decision-making process of downstream users of the information.

It is also important that the DHP and points of service communicating with the DHP also prevent updates to records containing clinical data, or data upon which clinical decisions have been made. Once submitted, signed data should be considered unalterable, and changes should be submitted as amendments (or versions) to the original. This allows appropriate tracking of changes over time, to understand the basis upon which historical clinical decisions were made.

3.2.4.2 Timely

When patients transition between facilities, or care settings there is be a need for the DHP to facilitate

[20] National Digital Health Guidelines and Standards [2] Section 3.1.10

[21] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5961786/

the exchange of this data. Whenever business processes cross organisational boundaries, it is vital that requisite data is available to the receiving organisation to ensure uninterrupted care to the patient. Use cases where timely access to information is of elevated importance are:

- Digital capturing of physician order entries, currently BHTs (Bead Head Ticket) at ward level to EMRs
- Transfers between facilities (such as a routine care to an emergency care centre)
- Sharing of medical imaging between facilities
- Requests to laboratory facilities and pharmacies
- Specimen collection, shipping, and lab testing
- Diagnosis of communicable diseases for outbreak management
- Notifiable communicable diseases

This timely delivery of data requires that the DHP be available to all points of service. The nature of using internet communications technologies will ensure that data about the patient is available in a near-real time manner (i.e., in a matter of minutes rather than days).

3.2.4.3 Complete

When a request is made to the DHP from points of service, it is important that the data presented back to the requesting provider is complete in nature. This means that the DHP (and by extension, the point of service) must ensure that all data available for the requested recipient of care is disclosed. Any summaries produced by the DHP or NEHR should include links to the original sources of the summary information.

If portions of the clinical record for the client cannot be retrieved due to privacy directives, lack of access credentials, or other infrastructure or application issues, it should be clearly identified to the consumer of the information.

In some care settings where time sensitive access to information is required (such as emergency care, paramedic care, etc.) the DHP should not block information where blocking it would inhibit care and should provide an override mechanism for specifying purpose of use (i.e., the point of service is requesting access to patient data for EMERGENCY purposes). Such requests where sensitive information is disclosed to the provider should be appropriately audited and logged.

In cases where the patient’s identity has been associated with a policy which prevents recordation of or disclosure of data (such as an opt-out) or where data had previously been registered and subsequently removed (such as a withdrawal of consent) the DHP should provide an indication that data is missing from the result set.

3.2.4.4 Requirements

- The DHP shall define methods which allow for the validation that information submitted to a patient’s NEHR is accurate, reviewed by a responsible person/organisation, and are unaltered.
- The DHP shall define methods which allow for the amendment of clinical data (clearly identifying the history of amendments) and should, prevent direct modification to data within the patient’s NEHR once signed.
- The DHP and its services shall be accessible in a manner which allows all authorised and relevant parties to query for data from the patient’s NEHR.
- The DHP shall define reasonable timelines and timeframes (based on trigger events) for which summary data from events are to be submitted.
- The DHP and connected services shall provide notice to consumers of information whenever data returned to a point of service represents an incomplete set of results (masked, redacted, etc.) as well as the status of results (preliminary, unconfirmed, entered in error, etc.)

3.2.5 Provide Secure and Private Access to Health Information

The primary goal of the DHP is the establishment of a nationally scoped, patient centred, electronic health record. This necessitates the storage of discrete personally identifiable health information (PHI) which is sensitive by nature. Combined with the ever-increasing nature and sophistication of cyber security threats online, it is important that all data and participating systems within the DHP are protected.

It is important that, prior to integration with the DHP, all digital health services undergo appropriate security audits to ensure that the software and deployment adhere to minimum standards set forth in blueprint[22].

3.2.5.1 Secure

The notion of security within health software has a few key attributes which extend to the DHP, and all solutions integrating with the DHP. These are:

- *Encryption of data in transit:* Whenever data is moved from one system boundary to another it must be encrypted using industry standard encryption algorithms (i.e., RSA + AES). Typically transport layer encryption (such as HTTPS, SLLP, SFTP, etc.) is sufficient for the protection of data in transit. There are certain use cases where encryption of data at the application level (i.e., payload encryption) will also be used when data from one sensitive sender needs to transit the DHP to another sensitive receiver (the DHP will not inhibit such transactions).
- *Encryption of data at rest:* Whenever data is stored on shared infrastructure, it must at minimum, be encrypted on durable storage media. There are several mechanisms which should be used for this purpose:
  a. Disk level encryption: Where virtual disk drives or drive images are encrypted. These prevent physical theft of disk devices from being breached.
  b. Database level encryption: Where sensitive database tables, columns, or fields are encrypted when stored on the disk. This type of encryption ensures that if the host operating system is breached, the database contents cannot be dumped.
  c. Application encryption: Where the applications or APIs will make calls to cryptographic APIs to manually encrypt sensitive data such as image files, logs, text files, and even database data.

The sensitivity of data being stored, and the intended use will dictate which encryption at rest strategy is used. Key management is also important to encryption of data at rest.

- Access Control: Whereby access to certain systems, functions, or even data is blocked. Using either:
  a. Role Based Access Control (RBAC): Where the decision to grant or deny access to a function, or data is made based on asserted roles which the user holds in their current session credential, or
  b. Policy Based Access Control (PBAC): Where the decision to grant or deny access to a function or data is made based on a combination of roles the user holds, policies on the action/data, configuration of the environment, etc.

The decision and behaviour of each PoS and administrative interface within the DHP is not specified in the blueprint, so long as minimum security considerations outlined in the interoperability profile is fulfilled.

3.2.5.2 Private

With the introduction of a, DHP it will become easier than ever before to collect, store and analyse large

[22] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5961786/

sets of data about individuals. Personal Information (PI) is generally considered to be information about an individual that is recorded in any form which can be used to uniquely identify an individual (such as name, address, etc.). Collection of such data brings benefits to citizens, however also introduces potential privacy risks through misuse.

Protecting the privacy of personal information is a legal requirement under The Personal Data Protection Act – March, 2022[23], which sets the legal framework within which the privacy of health clients and providers must be protected.

3.2.5.2.1 Personal Data Protection Act, Sri Lanka

On March 18th, 2022, Sri Lanka enacted the Personal Data Protection Act, No. 9 of 2022 (the "Act" or "PDPA"), a comprehensive data protection legislation modelled after the General Data Protection Regulations (GDPR) in the EU, and gradually comes into effect in the beginning of 2023.

The Act applies to any processing of personal information that takes place in Sri Lanka, which applies to processors and controllers[24] that offer goods or services to persons in Sri Lanka. The PDPA Act relies heavily on GDPR's principles of legitimate purpose, proportionality, and transparency, among others. Under PDPA data controllers and processor (i.e. the DHP components, MOH, etc.) must ensure that processing of personal information utilises the following principles:

- *Legitimacy:* Processing of personal information must be for a "specified, explicit and legitimate" purpose.
- *Proportionality:* Processing of personal information must be "adequate, relevant and proportionate" to the extent necessary in relation to the purpose of processing.
- *Accuracy:* Processing of personal information must be "accurate and kept up to date".
- *Limited Retention:* Personal information should be kept only as far and as long as necessary for purpose to which it was processed.
- *Integrity:* Controllers must ensure integrity and confidentiality of personal information processed by using appropriate technical and organizational measures including encryption, pseudonymization, anonymization, access controls or other such measures.
- *Transparency:* Controllers have an obligation to process in a transparent manner enabling data subjects to receive information they request regarding the processing of their information.
- *Accountability:* Controllers must implement internal controls and procedures, a "Data Protection Management Program", to maintain adequate data processing records and ensure appropriate oversight.

Under PDPA, data subjects have the following rights and choices:

- *Right of access:* Data subjects have the right to request access of their personal information.
- *Right to withdrawing consent:* Data subjects have the right to withdraw consent and to object to the processing of their personal information.
- *Right to rectification:* Data subjects have the right to request that their personal information be corrected or rectified when inaccurate.
- *Right to erasure:* Data subject may request to have their personal information erased.

Periodic monitoring by the minister (an Adequacy Analysis) is performed to ensure compliance. The act also provides protections and guidelines for the transfer of data outside of the territory of Sri Lanka, whereby electronic processing of data outside of the territory must be reviewed. Additionally, organisations which process health information are required to appoint a data protection officer (DPO) who advises the organisation on appropriate requirements for protection of personal data and ensures compliance using threat risk assessments

[23] PL 012913 Personal Data (Act) Cov.pmd (documents.gov.lk)
[24] GDPR data controllers and data processors (gdpreu.org)

and personal information protection impact assessments.

3.2.5.3 Requirements

- The DHP shall provide a method of conveying user identity assertions within the infrastructure to allow for granular security and privacy enforcement decisions.
- The DHP shall govern the creation, update, disclosure and deletion of data within the shared health information environment according to configured policy directives (examples: do not store data/opt-out, emergency use only, etc.)
- The DHP shall maintain a centralised audit trail which allows for compliance audits, security or data breach detection.

3.2.6 Streamline Clinical Data Collection for Secondary Uses

Digital health data captured from points of service present a unique opportunity for secondary uses. Whether supporting research, product recalls, or financial and resource planning, secondary use of data within the context of the DHP are of the utmost importance. The DHP will provide a health information warehouse which stores aggregate level data for secondary uses and will provide facilities for creating data warehouses, repositories and other data marts which can be used for data mining, decision support and other applications.

For example, the DDG Planning Unit may use transactional data within the DHP to determine how to best deploy financial resources based on district discharge summaries (indicating hospital uses). The DDG MS I unit may use the same data to determine the appropriate staffing levels for medical officers within facilities of a particular district.

The DHP supports the generation of KPI (key performance indicator) measures by:

- Using transactional data to generate measurements either:
  a. Observing Transactional Data within the DHP and relaying indicator measures to a health information warehouse as they occur.
  b. Allowing processes to query aggregates from the DHP services using queries on APIs to obtain measure counts.
- Direct reporting of aggregates from health institutions by (example eIMMR – electronic indoor morbidity and mortality register):
  a. Allowing for the dissemination of KPI definitions, reporting cadence and requirements to institutions.
  b. Providing services for health institutions to submit computed indicators directly to a health information warehouse for specified reporting periods.

The information contained in the DHP's health information warehouse should be sufficient to support all activities of the MOH administration including:

- Use by DDG Planning to allocate investment, plan service delivery, outreach activities, etc.
- Use by the DDG MS-I and MS-II units to provide and plan for appropriate staffing levels.
- Use by DDG PHS-I and PHS-II for population's health monitoring and interventions, within the MOH.
- Use by MOH to generate health systems reports which are submitted to international bodies for reporting, and health systems reporting
- Use by researchers and research institutions including to evaluate the efficacy and cost of new health interventions.
- Use by medical safety regulators to evaluate drug adverse events, medical device failures and coordinate/investigate potential recalls of products.
- Use by central and provincial public health authorities to monitor communicable disease outbreaks.

The health information warehouse should support open data exchange standards, standard terminology services and definitions for datasets collected and reported. This exchange of aggregate KPI data from the DHP will foster research use and innovation among any authorised parties within the Sri Lankan health system and to create custom dashboards visualisations of data. And research papers.

As with all data stored within the DHP, the provenance and validity of these KPI should be tracked. This means that any aggregates generated from transactional data should link to the data event from which the measure was computed. Any KPI measures submitted in aggregate from source should have mechanisms in place to ensure validity and review status from the submitting organisation.

3.2.6.1 Requirements

- The DHP must provide a health information warehouse which stores aggregate level data for secondary uses. The information warehouse should:
  a. Provide a mechanism for establishing data marts for particular purposes
  b. Support the storage of discrete data elements (pseudonymized for protection) or aggregate indicators
  c. Support data mining activities such as Online Analytical Processing (OLAP) data cubes, data lakes, or other statistical analysis tools
- The DHP must provide a facility which allows planning units to define and share KPI definitions for which they expect organisations to submit regular reports.
- The health information warehouse must provide a link to original source data (if generated from DHP transactional data) or provide a function to ensure that aggregates were validated by a source organisation.
- The DHP must provide an open API for aggregate data in the health information warehouse, allowing for development of custom dashboards, research, and visualisations of data within the DHP and at sub-national, institutional ad unit levels, as required.

3.2.7 Enhance Operations of Ministry of Health

The MOH, its DG and DDGs represent a large contingent of directors, administrators, clinicians, and support staff. The dissemination of and effective use of resources is of utmost importance to ensure that business services are delivered in a consistent, cost-efficient, and adherent manner.

Examples of opportunities for leveraging digital services for the enhancement of operations within the MOH include:

- Providing official ministerial e-mail addresses to government staff members, ensuring that communications between staff, staff and patients, or administrators is stored in a manner which can be protected and monitored.
- Providing single sign-on services between applications used within the ministry of health. Since staffing transfers and management is performed by the various DDGs (for example: MSI and MSII) central policy application and consistent identity for auditing and logging tracking would greatly improve monitorability of the DHP services, as well as provide users with a simpler experience when using digital health services.
- Dissemination of new policies, circulars, training materials and other administrative documents to staff. A central document management solution would provide the ability to quickly share and handle document assets (with consistent referencing) within the organisation.
- Enterprise knowledgebase development allowing of the collection of institutional standard operating procedures, frequently

asked questions, and directing staff (and patients) to appropriate digital health resources within Sri Lanka.

- Enterprise issue ticketing to facilitate the collection, tracking, and resolution of issues related to review of documents, transfer requests, technical issues, and improvement requests. Including help-desk escalation processes.
- Human Resources management, allowing for the processing and allocation of staff within the Sri Lankan public health system. The current use of the Human Resources Information Management System (HRIMS) should be integrated into the digital health platform solution.
- Logistics and supply management via consistent processes and channels, migrating away from manual processes via integration of various clinical systems and moving towards automated techniques as DHP services mature.
- Enterprise Project Management and lifecycle tracking for measuring and planning the implementation of physical and digital health interventions within the health enterprise.

The DHP should consider the implementation of technologies which enhance the operational structure of the MOH and providing shared administrative resources.

3.2.8 Integrate Information Flows Within the Enterprise

The digital health environment within Sri Lanka contains many disparate systems which are at various stages of scale up and scale out. Currently, many of these systems are silos of information along disease verticals, or clinical setting with limited data exchanges for discrete patient care delivery data.

A key driver of a digital health exchange is the ability for different organisations to exchange data to better serve patients. Currently, implementations of the Hospital Information Management System (HIMS/SWASTHA) and Hospital Health Information Management System (HHIMS) are locally installed and neither connected with each other nor among their own instances, even though there are business processes and information flows which would benefit hospitals and patients running these solutions such as:

- Ensuing mobility of patient records across hospitals making them available at points of care
- Transferring of patients between facilities for clinical reasons (i.e. to specialist hospitals or base hospitals to apex hospitals)
- Alerting hospitals of the availability of live donors from ICU and/or matching current transplant recipients.

The integration of information flows and business processes is not limited to single types of care settings. Although there is likely no need to interconnect every system in use, there are chronic and communicable disease use cases where the integration of information between disease programs would provide a high degree of benefit for clinicians. Examples include:

- Integration data across disease programs where co-morbidities are important (example: integrating eIMS, operated by NSACP for tracking HIV patients and ePIMS, operated by TB & Chest, for tracking TB)
- Sharing curative care records and displaying along with public health care records where necessary
- Coordinating care for chronic conditions between hospitals and primary care settings such as transplant recipients, cancer treatment recipients, patients with diabetes, and more.
- Relaying hospital discharge and admission information to disease care providers such as general practitioners

3.3 Proposed Future-State

The solution proposed to fulfil the needs of the DHP in Sri Lanka are illustrated in Figure 9 and is described in more detail in section 3.

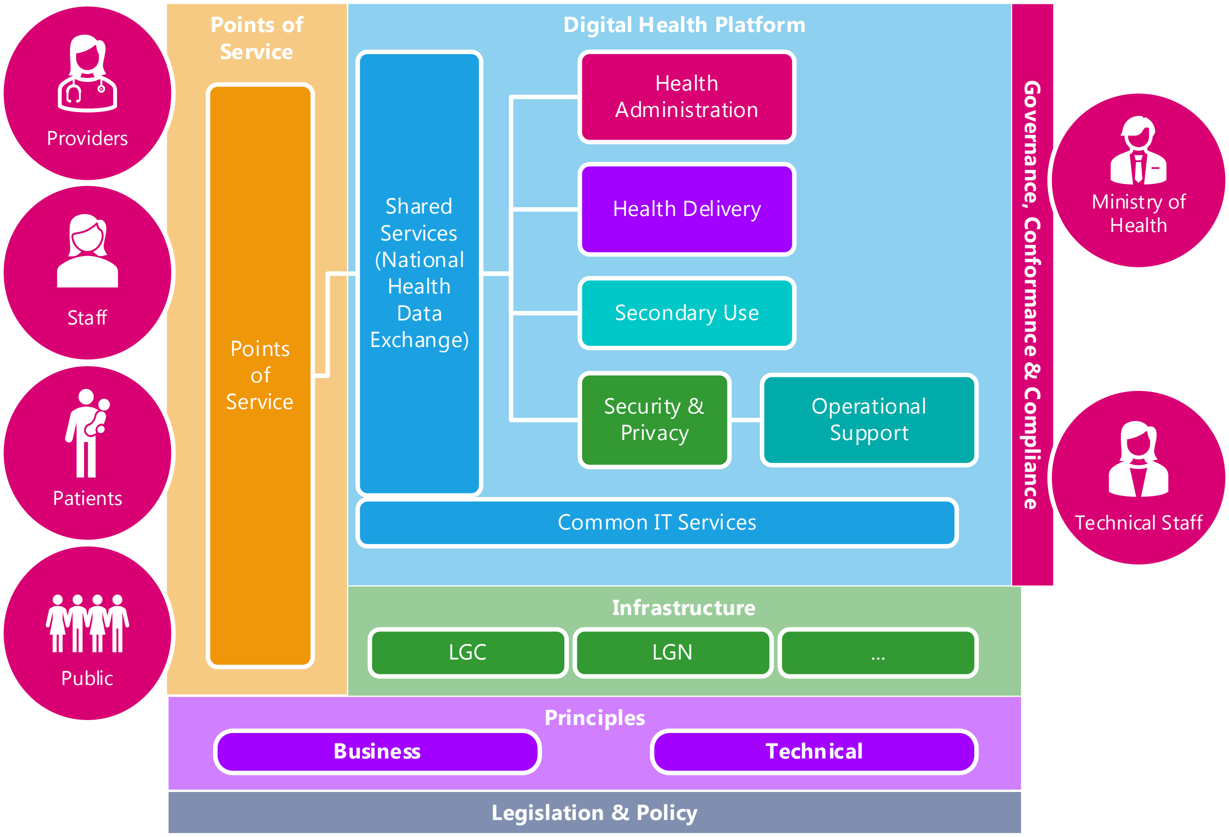


Figure 9 : *Proposed Future State Domain Relationships*

The solution allows for existing systems at points of service (PoS) to consume and contribute data with a centralised infrastructure. The term PoS encompasses any solution:

- Used by care providers (EMRs, HIS, etc.)
- Used by patients (personal health records, etc.)
- The general public (informative websites, public health sites, etc.)
- Administrative staff (HRMIS, planning tools, transfer and capacity planning, etc.)

The blueprint and digital health platform enhances the current state business architecture by supporting and enhancing current operations as illustrated in Figure 10.

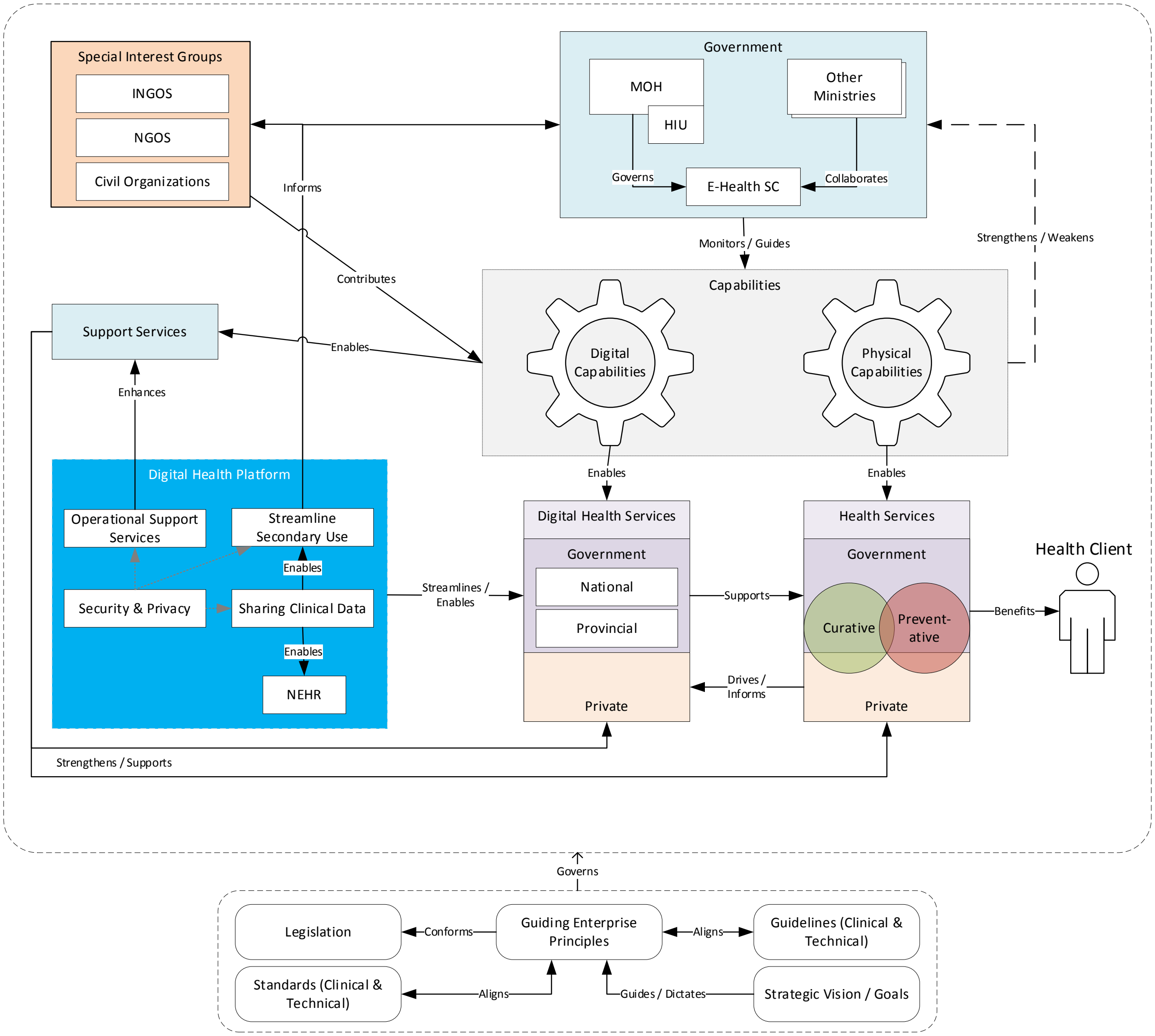


Figure 10 : *Enhanced Future State*

3.3.1 Proposed Solution Outcomes

The proposed future state solution has been created to meet the needs of the target business drivers described in section 3.2. The solution meets these drivers as it:

- Establishes of a nationally scaled, electronic health record for all patients in Sri Lanka, including relevant data from public institutions and private institutions.
- Establishes interoperability between clinical and preventative health information systems (points of service) via a centralized integration technology.
- Establishes common vocabulary, terminology and data services and standards within the health sector.
- Establishes registries and supplemental services for patients, facilities, providers, commodities, drugs, and other entities referenced within the health sector.
- Establishes a platform to support shared care and referral services between government and private sector care delivery settings.

- Establishes shared messaging services (via operational support services) between providers and clients.
- Establishes a platform for more consistent and rapid capacity building via dissemination of enterprise knowledge artifacts.
- Improves the ability to perform analytical processing a planning via the establishment of a national digital health information warehouse.
- Establishes a common infrastructure for SMART health systems using shared clinical decision support (CDS) services.
- Establishes a common infrastructure for the requisition/order and tracking of drug, supplies, equipment between local, provincial and national levels.
- Provides mechanisms for issuing centralised application API keys, allowing for the evaluation and enlistment of new digital health applications into the ecosystem.
- Ensures that disclosure and exchange of health information is ethical and patient privacy is protected and/or audited for monitoring and compliance purposes.
- Ensures the security of health information by providing central control of disclosure policies and access policies in the DHP.
- Fosters digital health research (allowing for secure and private data for secondary uses) and innovation (allowing for a common platform upon which new interventions are developed).

3.3.2 Managing Complexity

The DHP manages the technical complexity identified in section 3.2.1 by defining a solution based on the principles of Services Oriented Architecture[25]. This approach breaks complex solutions into component services which can be re-composed to accomplish different business goals. By following this approach, the complexity of the solution can be mitigated by:

- *Enabling an Evolutionary Approach:* Services and problem domains can be defined using a consistent process using the blueprint as a framework for establishing the solution and technical view for each specific problem domain. This means that the DHP will grow incrementally over time, allowing providers, implementers, and patients to adapt to each change incrementally.
- *Using Standard Approaches:* To maximise service solution reuse, allowing implementers and integrators, over time, to focus on value-add capabilities of the DHP rather than wasting time performing one-off integrations and mappings.
- *Service Encapsulation, Coupling and Cohesion:* By defining common problems within the enterprise, and designing the units with high degrees of cohesion we can ensure that DHP remains loosely coupled allowing for incremental growth and change.
- *Re-Use of Services:* By ensuring that services expose atomic business functions in the DHP, it is possible to re-compose services to orchestrate solutions for different workflows and use cases.

3.3.3 Interoperability

The NEHR business driver must be built on the foundation of interoperability to ensure that data and processes are standardised between organisations, software solutions and care settings. This requires not only technical interoperability, but also organisational interoperability (to ensure processes across organisational boundaries).

Interoperability within the health domain is complex. Health encompasses a wide variety of data structures (images, video, structured data, documents), clinical and business processes (de-

[25] Erl, Thomas - SOA Principles of Service Design, ©2008, Prentice Hall ISBN 0-13-234482-2

duplication, merging, order flows, etc.) as well as privacy, security and governance requirements. All of which must occur in a semantically consistent manner to ensure exchanges of health information are reliable, and safe[26].

Work has already been performed in the National Digital Health Guidelines and Standards (NDHGS) document to establish baseline interoperability guidelines. These are further elaborated and specified in more detail in the accompanying interoperability plan and forthcoming interoperability profiles. At a high level, interoperability within the blueprint focuses on:

- *Foundational Interoperability:* Establishes the baseline connectivity such that one application can securely and consistently communicate data to another application via a baseline set of interchange protocols (FTP, HTTP, etc.)
- *Structural Interoperability:* Establishes common, minimum data elements are captured in a consistent manner. This is often realised using common interoperability structures (such as HL7 FHIR, DICOM, etc.). The National Digital Health Guidelines and Standards[2] sets forth guidelines for the data elements to be captured by digital health solutions. These elements should be adapted and referenced in logical views.
- *Semantic Interoperability:* Establishes the "meaning" of the clinical data is understandable not only between computer systems, but business units and their staff. Semantic interoperability is of the utmost importance and the assets of the blueprint should establish a collective understanding of the data. For example, defining a KPI "number of planned school outreach programmes" may be ambiguous depending on the province, software vendor, or business unit which is reporting these values.
- *Process Interoperability:* Ensures that the "actions" which should be taken by systems and organisations within the enterprise are clearly articulated and understood. Defining common and acceptable triggers for interacting with the DHP is a key consideration of the solution to ensure that each software solution, business unit, and province behaves is a consistent manner. For example, the conditions under which client information should be updated in the national client registry (i.e., at birth, at death, primary residence change, etc) and the expected actions of connected systems.

The Lanka Interoperability Framework (LIFe) defines a set of open standards with the goal of facilitating interoperability between government information systems. LIFe currently identifies baseline standards for Land, Personal, Vehicle and Project Coordination domains[27]. The adoption of international standards for use in Sri Lanka within the health domain should, where possible, adapt the definitions and constraints on data elements specified in LIFe. Standards and profiles developed to support the DHP should also, where possible, be included in the LIFe catalogue of standards.

3.3.4 Scalability

Scalability can be described using several dimensions[28] which can be applied to enterprise integration environments. Using SOA design patterns, the DHP solution ensures that there is ample opportunity to scale the DHP across these dimensions. This section explores how the scalability considerations for the DHP are addressed in five areas:

- *Generational Scalability:* The ability of the DHP and its services to absorb and adapt as new standards, innovative technologies, or business units become available, without impacting previous services.

[26] Interoperability in Healthcare | HIMSS

[27] LIFe - Lanka Interoperability Framework

[28] Advanced Computer Architecture and Parallel Processing - Hesham El-Rewini, Mostafa Abd-El-Barr - Google Books – Pg 66

- *Geographic Scalability:* The ability of the DHP and its services to grow to support new geographic regions and their related governance and access requirements.
- *Heterogenous Scalability:* The ability of the DHP and its services to operate in an environment where a variety of open source and proprietary software systems reside, on a variety of platforms.
- *Administrative Scalability:* The ability of the DHP and its services to grow to serve more organisations and users in a manner which does not overburden or detract from existing users or organisations.
- *Functional Scalability:* The ability of the DHP to add or onboard new business functions without disrupting existing business functions.

3.3.4.1 Generational Scalability

The separation of the blueprint into views ensures that the DHP specifications can be adapted to support new technologies, standards, and processes as they become available. For example, by specifying the functionality of the NEHR Repository as business triggers, data elements, storyboards, etc. the NEHR can be realised in FHIR, however if a new technology or standard becomes available (HL7 Version 5 for example), the same business functions can be realised in this new standard as a separate technical view.

Additionally, the use of an enterprise application integration architecture allows the DHP to support the adoption of new technologies while isolating clients from these changes. This permits the adoption of innovative technologies such as virtual reality, remote surgery, or digital pathology without destroying or changing connections with points of service. To maintain generational scalability, physical realisations of integration components (such as the data exchanges, shared infrastructure, security services, etc.) should not assume a “FHIR only” environment. Heterogenous standards environments using SYSLOG, XML, HTTP, DICOM, and LLP are usually required and the DHP should permit the onboarding of these technologies.

3.3.4.2 Geographic Scalability

It is important since the DHP be designed in a manner which permits sub-national scaling operation of certain services. Common use cases for this type of scaling are:

- Sub-national jurisdictions managing access credentials for users which they have hired without the need of central administration doing so.
- Sub-national jurisdictions managing their own reference lists for indicators, human resourcing, or other permitted policies as appropriate, without the need of central administration.
- Scaling of the NEHR to support performance scaling of the repository service.

The DHP proposes the separation and federation of services within the DHP at a component level. The decision of which components are scaled (such as the NEHR Repository, Imaging Repositories, etc.) will depend on the workload and storage requirements of each geographic area. Whether this is scaling is performed at a physical level (i.e. separate servers), instance level (i.e., separate virtual machines) or at a software/data level (i.e., application or database scaling) is not specified here and will depend on the capabilities of the software component in question.

3.3.4.3 Heterogenous Scalability

The underlying foundation of the proposed solution is based on an open architecture[29] which permits the scaling of the DHP over time within a heterogenous manner by defining the behaviours

[29] Clifton A. Ericson, II - Concise Encyclopaedia of System Safety: Definition of Terms and Concepts. © 2011, John Wiley & Sons. p. 272. ISBN 978-1-118-02865-0.

and interfaces in a standard manner. The blueprint must support consumers of providers of DHP components can be implemented and realised by a variety of vendor solutions, which should have no impact on the functioning of the overall DHP.

While the blueprint encourages the use of open-source technologies, use of proprietary (free or commercial) technologies may be required. The blueprint makes no assumptions about the nature of each component, and therefore must support a heterogenous environment.

This open architecture is important as:

- It allows new software solutions to be swapped in or out of the DHP based on support lifecycles, technical evolution, or applicability.
- It fosters innovation by allowing private sector vendors as well as open-source communities to compete with one another in a consistent framework.
- It prevents vendor lock-in and platform lock-in (i.e., a Java/Tomcat based solution can be swapped with a .NET/IIS solution if appropriate, or vice-versa)

3.3.4.4 Administrative Scalability

The digital health platform is designed to foster onboarding and growth over its lifetime. Using open architecture and specifications - new institutions can be onboarded to the shared DHP infrastructure without impacting existing institutions.

The administrative burden of onboarding a new institution should involve little more than registration of the institution's security certificates (public/private key pair) to access NHDX services and setting appropriate application credentials.

The operation support systems identified in the DHP solution are designed to assist in the administrative scale-up of the DHP solution. Document management systems to disseminate Standardised Operating Procedures (SOPs), setup of an enterprise knowledge base, central learning management system, and issue/helpdesk ticketing solutions should be deployed and leveraged for each domain in the DHP. Having consistent materials linked and referenced in the DHP ensures that, across the enterprise, new organisational and human users can be trained efficiently.

3.3.4.5 Functional Scalability

Functional scalability ensures that new operations and components (or functions) can be added to the solution without impacting or changing existing functions.

- *Encapsulation:* Each service provided by the DHP, should expect to receive all data and trigger event information required to perform the desired business function. There must be no assumption that a target or consumer of data "knows" information not included in the interaction. The receiver should store and faithfully reproduce data which it has received.
- *Loose Service Coupling:* Each service within the DHP is loosely coupled. Each service should not have hard coded dependencies on another service provider which is not documented in the DHP. Loose service coupling ensures that if a function is missing, replaced, or deprecated, that other services should continue to operate without hindrance.
- *Service Cohesion:* Each service should support a high degree of cohesion, meaning that the service should implement only those functions and operations within the enterprise for which they are the appropriate business module. For example, the job of matching and merging patients should be implemented within the Client Registry software, rather than a shared health record.
- *Evolutionary Growth:* Each service should be maintained and implemented in a manner whereby new functions and API endpoints can be added without changing or breaking previous functions. This can be done via

normative code changes on access points. If new functions need to be deployed which modify previous behaviour, they should be exposed on new access points.

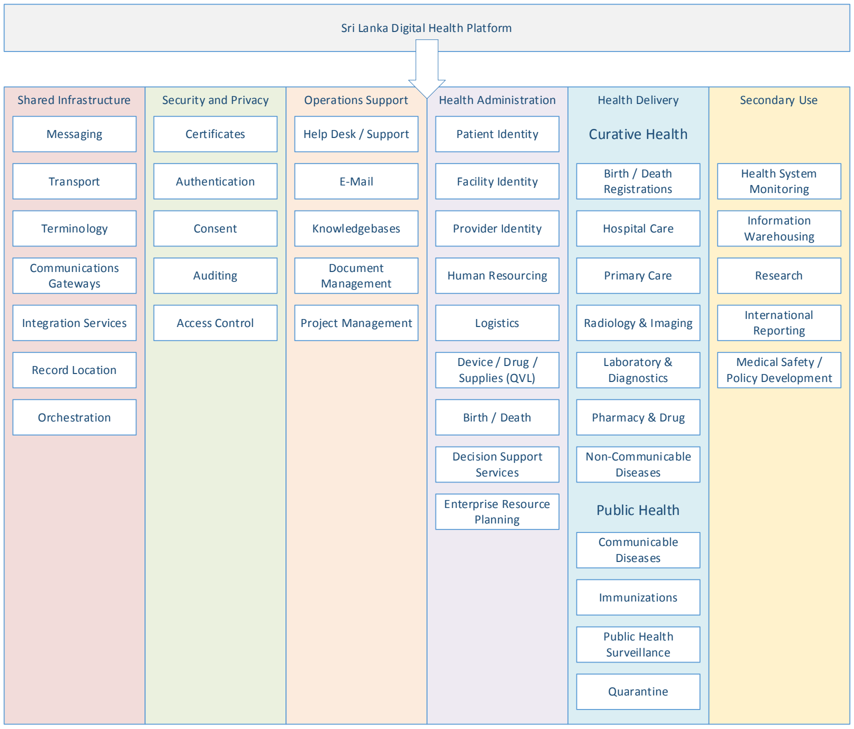
By implementing these attributes, the DHP in Sri Lanka can be expanded to support new clinical domains (example: implementing a cancer care repository, or donor/transplant matching services), onboard new or existing applications, or integrate new functions.

3.3.5 Blueprint Architectural Domains

This section defines and discusses the logical problem domains of the DHP. The blueprint seeks to assist in the organisation of workgroups for further development of the platform by separating concerns in a series of business domains.

1. Shared Infrastructure: Which is concerned with the reliable transport, transformation, routing, and delivery of information within the DHP infrastructure.
2. Security and Privacy: Which supports the protection of the DHP data by specifying the authentication and identification of users and devices, encryption and signing, and consent.
3. Health Administration: Administrative concerns in the DHP. This encapsulates the identification of locations, providers, clients, supplies and logistical support.
4. Health Delivery: Concerned with delivery of curative and preventative clinical care. Encapsulates concerns related to indexing, storage/retrieval, and non-repudiation of clinical data.
5. Operations Support: This domain is concerned with the overall operations of the Ministry of Health and related stakeholders and includes helpdesk, communications, training, etc.
6. Secondary Use: Concerned with the use of data within the DHS for the purposes of public health monitoring, research, planning and policy development, and any other non-clinical use of data.

These domains contain further areas of concern which serve as the business case for components within the DHP.



Sri Lanka Digital Health Platform

Shared Infrastructure	Security and Privacy	Operations Support	Health Administration	Health Delivery	Secondary Use
Messaging	Certificates	Help Desk / Support	Patient Identity	Curative Health	
Transport	Authentication	E-Mail	Facility Identity	Birth / Death Registrations	Health System Monitoring
Terminology	Consent	Knowledgebases	Provider Identity	Hospital Care	Information Warehousing
Communications Gateways	Auditing	Document Management	Human Resourcing	Primary Care	Research
Integration Services	Access Control	Project Management	Logistics	Radiology & Imaging	International Reporting
Record Location			Device / Drug / Supplies (QVL)	Laboratory & Diagnostics	Medical Safety / Policy Development
Orchestration			Birth / Death	Pharmacy & Drug	
			Decision Support Services	Non-Communicable Diseases	
			Enterprise Resource Planning	Public Health	
				Communicable Diseases	
				Immunizations	
				Public Health Surveillance	
				Quarantine	

Figure 11 : *Business Domains and Functional Concerns of the Blueprint*

4. Application Architecture

4.1 Current State

The DHEAP included a conceptual classification of the systems and information flows in Sri Lanka and is included in Figure 12 for context of the reader.

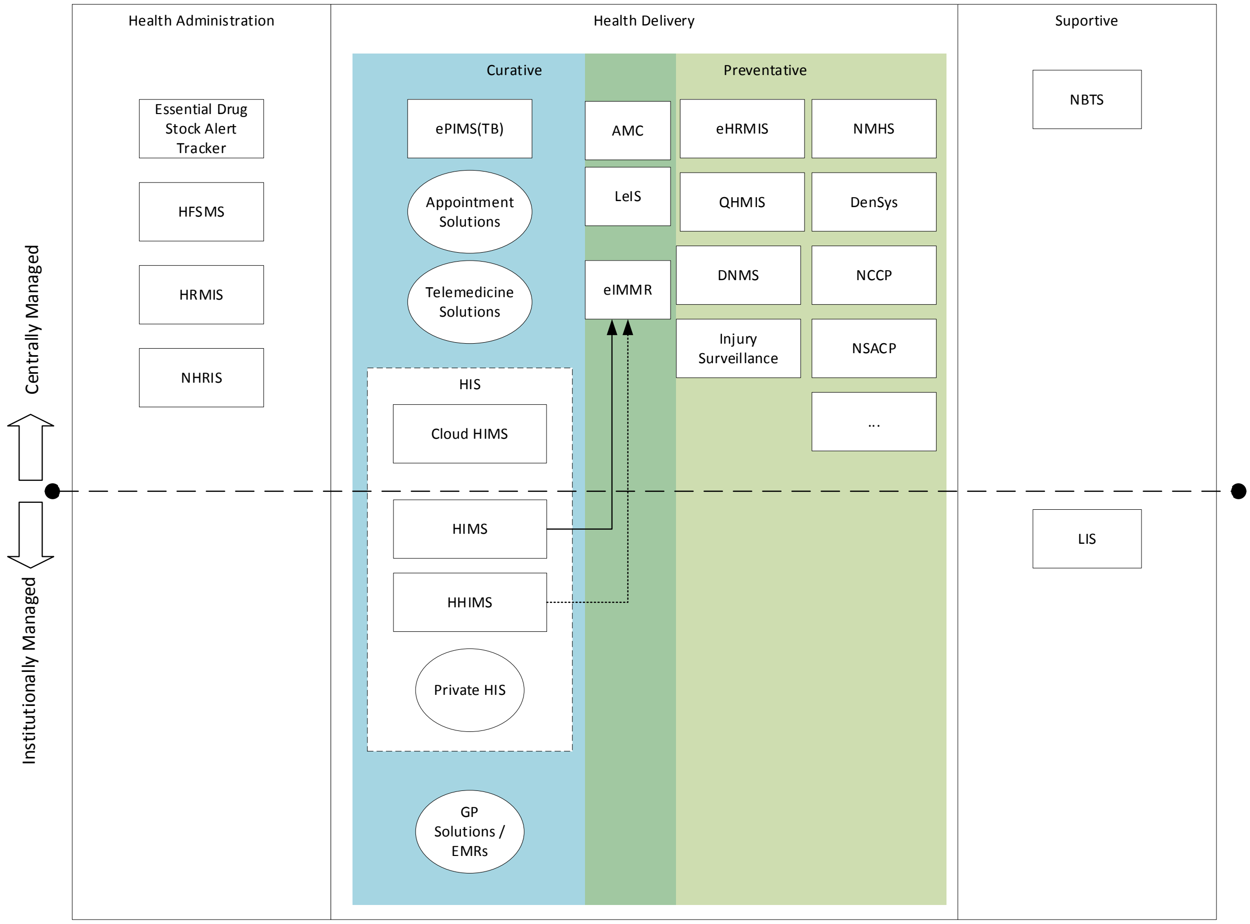


Figure 12 : *Current State Conceptual Architecture*

A complete list of abbreviations can be found in Annex C, however the abbreviations for Figure 12 are also provided here as a convenience to the reader.

List of abbreviations:

ALC: Anti Leprosy Campaign, AMC: Anti Malaria Campaign, Cloud HIMS: Cloud Health Information management System, DenSys: Dengue Sentinel Site Surveillance, DNMS: District Nutrition Management System, eIMMR: Electronic Indoor Morbidity and Mortality Register, ePIMS(TB): Electronic Patient Information Management System for Tuberculosis, eRHMIS: electronic Reproductive Health Information Management System, HFSMS: Healthcare Facility Survey Management System, HHIMS: Hospital Health Information management System, HIMS: Health Information management System, HIS: Health Information System, HRMIS: Human Resource Management Information System, NBTS: National Blood Transfusion System, NCCP: National Cancer Control Programme., NHRIS: National Human Resource Information Management System, NMHS: National Mental Health System, NSACP: National STD and Aids Control Program, Private HIS: Private Health Information System, QHMIS: Quarantine Health Management Information System.

These systems share little direct information flows between systems. The primary existing digital information flows identified were between the HIMS and HHIMS to the Electronic Indoor Morbidity and Mortality Register (eIMMR). Classifying these current state assets using the enterprise domains of the blueprint, the current state of the blueprint is illustrated in Figure 13.

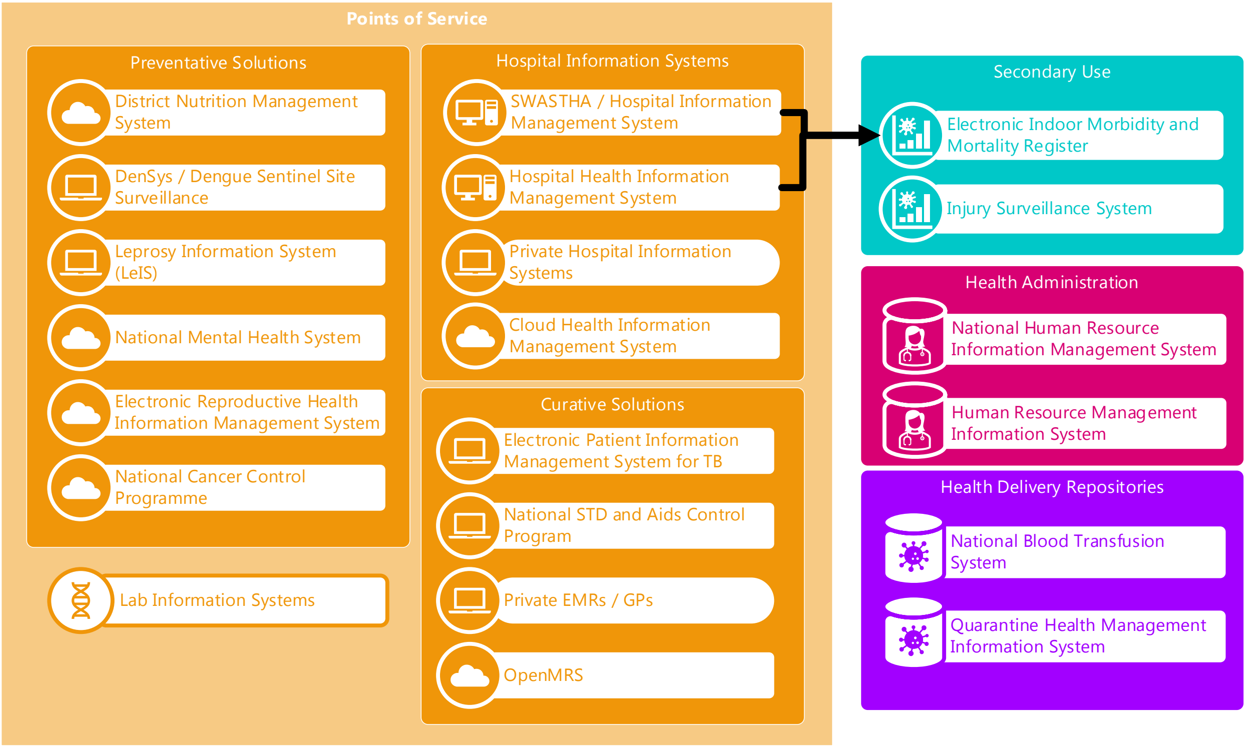

Points of Service
Preventative Solutions
District Nutrition Management System
DenSys / Dengue Sentinel Site Surveillance
Leprosy Information System (LeIS)
National Mental Health System
Electronic Reproductive Health Information Management System
National Cancer Control Programme
Lab Information Systems
Hospital Information Systems
SWASTHA / Hospital Information Management System
Hospital Health Information Management System
Private Hospital Information Systems
Cloud Health Information Management System
Curative Solutions
Electronic Patient Information Management System for TB
National STD and Aids Control Program
Private EMRs / GPs
OpenMRS
Secondary Use
Electronic Indoor Morbidity and Mortality Register
Injury Surveillance System
Health Administration
National Human Resource Information Management System
Human Resource Management Information System
Health Delivery Repositories
National Blood Transfusion System
Quarantine Health Management Information System

Figure 13 : *Current Application Architecture State (Blueprint Nomenclature)*

4.2 Proposed Future State

The proposed solution illustrated in Figure 14, is a refinement and further specification of the proposed architecture in Figure 9, on page 58 (a landscape oriented copy of this diagram is included in Annex E on page 156).

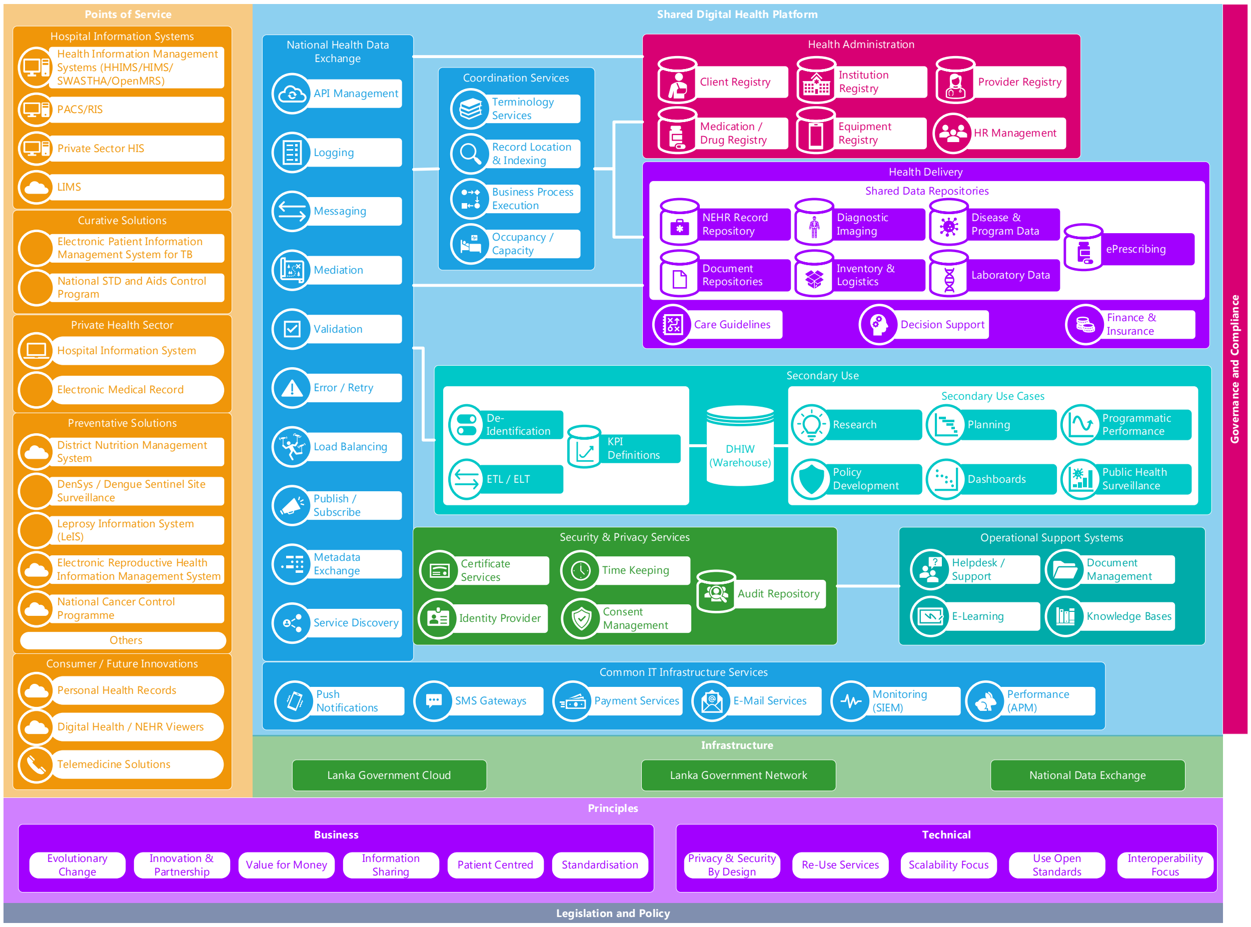


Figure 14 : *Conceptual Application Architecture*

4.2.1.1 Separation of Service Definition from Service Implementation

The documentation in the blueprint uses component definitions as the basis for functional descriptions and dependencies. The blueprint makes no supposition about the specific software products which will be used to implement the components and services described, rather it seeks to describe the functional role that each play within the DHP.

In the physical realization of this infostructure, multiple software packages can work together as a single logical DHP component, or a single software package can implement multiple functional components. For example: an API gateway, application firewall, and dedicated queueing solution may be combined to realize the NHDX.

Standards and integration patterns within the blueprint document are informative and are used to illustrate patterns the blueprint will leverage for information interchange. The Interoperability Plan and Interoperability Profiles are to be developed as supplemental documents which outline the detailed specifications for information interchange between components.

4.2.1.2 Infrastructure Diagrams

Diagrams in this section, and in the solutions views should exclude common infrastructure elements within the DHP (such as the NHDX, identity provider, SSL termination, etc.) to increase their readability and clarity. In the actual implementation, it is expected that all actors communicate using the common infrastructure and avoid direct communications with actors (even if the summary diagrams illustrate a direct relationship).

The intent is that the NHDX will assume the corresponding receiver role of the actor pair. For example, the actual actor relationships between systems could be as illustrated in Figure 15.

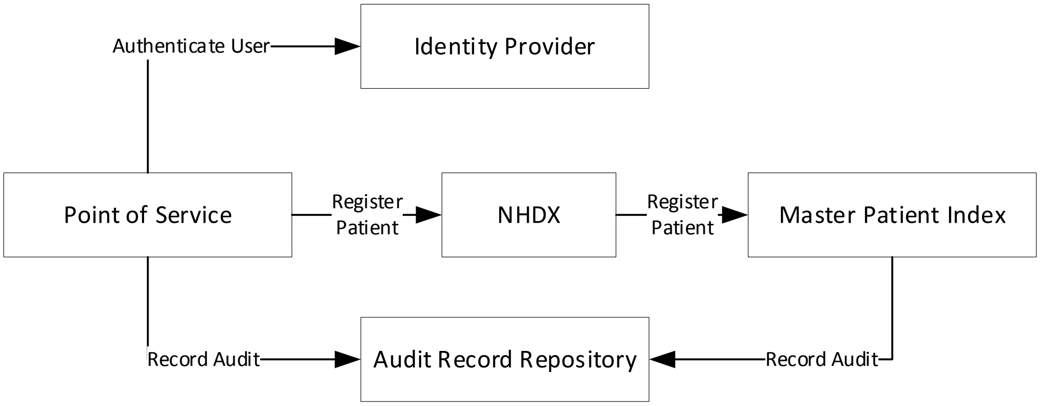


Figure 15 : *Technical Actor Relationships*

However, documentation will use a simplified form as shown in Figure 16, to clarify the intent of the diagram. Since the inclusion of the audit repository, NHDX, and identity provider are assumed to be omnipresent for all transactions their inclusion is not needed on all diagrams.

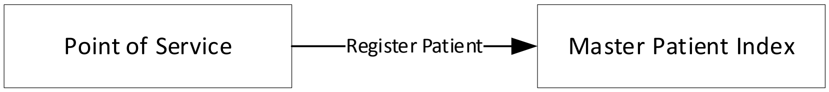


Figure 16 : *Simplified Actor Relationship*

4.2.2 Points of Service

The term Point of Service is used in the context of the blueprint and DHP to describe any application at which a user consumes services from the DHP (see Section 2.4.5 on page 30). This section describes the general considerations of points of service applications within the DHP.

Points of service represent the primary entry and viewpoint for data in the DHP. This means that special care should be taken when considering points of service for integration into the DHP:

- The DHP is only as secure as the weakest link, in the chain of trust. Software running within hospitals which are easily accessible physically represent a heightened security risk. Points of which interact directly with the blueprint architecture should be physically secured to prevent their removal.
- The lack of electronic medical records systems due to hardware failure is a serious threat to the smooth operation of clinical data capture and use. Efforts should be taken to ensure that appropriate backup hardware is available for end users of the DHP (including network, terminals and servers).

Like all components of the DHP, points of service are opaque to the blueprint. This means that the blueprint does not make any prescriptive architectural requirements of any one point of service, other than for its interaction with the broader health enterprise. Additionally, the points of service discussed in this section are exemplary, continuous development of digital health initiatives across Sri Lanka will continue to evolve and this list will become outdated.

4.2.2.1 Hospital Information Systems

There are many Health Information systems (HIS)in the country that belong to curative and preventive sectors. Also, within the same hospital there can be patient care Information systems for clinical care as well as managerial Health Information systems for administrative activity in the hospital. Further, there are number of Hospital Information systems related to clinical care of the patient in Sri Lanka. All such systems will make extensive use of the DHP, with many relevant use-cases of both retrieving and contributing information to the DHP. For example, the DHP can be used by the HIS systems to:

- Look up demographic and historical patient condition summary information in the DHP for patients during appointments and/or admission
- Retrieve last known medication lists and conduct drug-drug interaction checking during medication prescription
- Retrieve previous lab results and/or relevant diagnostic images
- Contribute admission notes, discharge summaries and referral notes

The DHP proposed by the blueprint augments the functionality of the already designed and implemented within these hospital systems. For example, the use of OpenMRS in multiple clusters with their own health services for patient management, data sharing between OpenMRS is envisioned to be unimpeded by the DHP. Rather, the DHP would augment these OpenMRS instances by allowing their connectivity to other solutions (such as Hospital Health Information Management System – HHIMS, or Cloud Hospital Information Management System - cHIMS). Additionally, the scope of data differs – whereas communication between OpenMRS instances primarily focuses on the OpenMRS dataset and use case (detailed hospital logs, detailed temperature, and care data), the DHP focuses on summary data for major events (such as a discharge, or referral between systems).

4.2.2.2 Curative Sector Solutions

Although HIS systems are also considered to be curative, additional curative systems exist in Sri Lanka, including the Electronic Indoor Morbidity and Mortality system (e-IMMR), and the Accidents and future proposed ones such as Telemedicine solutions Emergency Information System. As these systems are connected to the DHP and data begins to flow through the platform, opportunities exist to speed up the flow of information for health administrators. For example, near real time dashboards can be created to summarise data and reports in a fraction of the time that was previously taken. Opportunities to link data from different data sets will become available, offering new dimensions of analytics that were not possible in the future and will allow for the development of evidence-based policies.

4.2.2.3 Preventative Sector Solutions

Preventative solutions will interact with the DHP to contribute and retrieve valuable information for citizens and providers. Preventative solutions in Sri Lanka include the Electronic Reproductive Health Information Management System (eRHIMS), the District Nutrition Monitoring System (DNMS), the Electronic Mental Health Management Information System and the Web - based Immunization Information System (WEBIIS). For example, patients can be linked by a Master Patient Index inside the DHP so that care providers can receive meaningful submissions of data from all these systems and have it linked into a single longitudinal view of the patient.

4.2.2.4 NEHR Viewers / Personal Health Records (PHR) Systems

In the future, given appropriate consent, it will be possible for patients and providers to use DHP viewers which will retrieve, and display all known longitudinal information about a patient in a single view. Specialised "Apps" can be created to make use of the standardised data and provide intelligent in-context analysis and notifications based on patient metrics.

4.2.3 Shared Infrastructure

The shared infrastructure domain is described in Figure 17 and specified further in this section. For reference, the components of the conceptual architecture included in shared infrastructure domain are illustrated in Figure 14.

Shared infrastructure domain primarily addresses concerns with:

- Ensuring messages delivered to the DHP are reliably executed, retried, and tracked, ensuring that transactions are not executed twice on retry, relaying errors, etc.

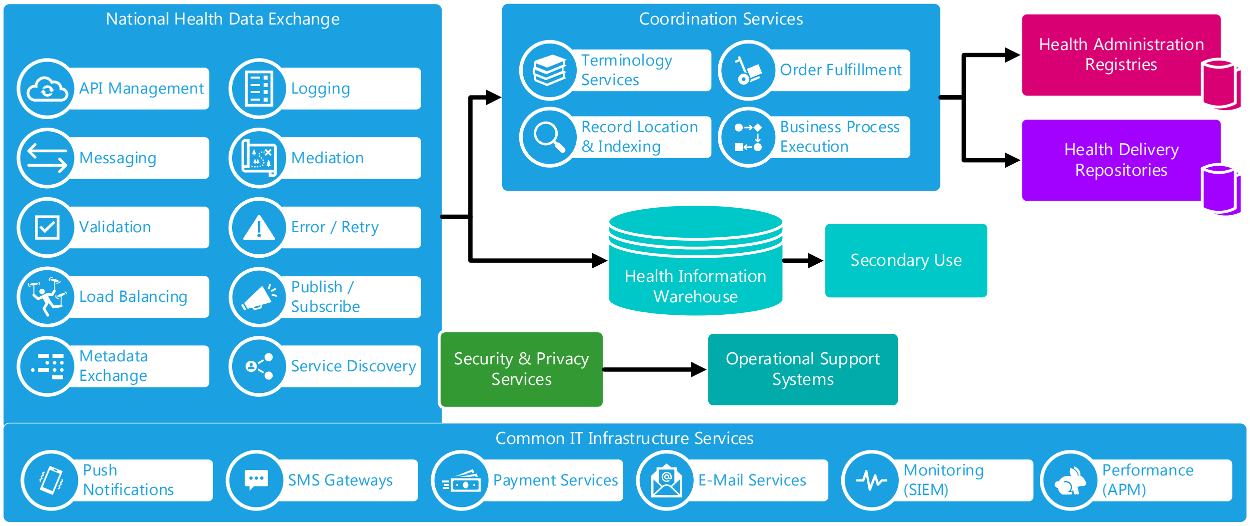


Figure 17 : *Shared Infrastructure Components*

- Services which ensure that the semantic meaning of messages are understood by all digital health services operating within the DHP.
- Communications gateways and common infrastructure for sending notifications to administrators, clinicians and providers including SMS, push notifications and e-Mail gateways.
- Transportation of messages to/from data services including proxying, message relays, etc.
- Service coordination:
  a. Business process execution allowing for complex workflows to occur within the DHP
  b. Terminology resolution, definition, validation, and mapping.
  c. Establishing linkages between orders (request for something), promises (intent to act), and fulfilment (event occurrence) which cross boundaries.
- Error reporting and retry of failed messages
- Enterprise service bus functions such as publish and subscribe management
- Access logging and basic API access control

In Sri Lanka, many of these services within the domain of shared infrastructure is provided via the Lanka Government Cloud (LGC) and the Lanka Government Network (LGN). Additionally, ICTA provides a national data exchange (NDX) which provides additional support for messaging, interaction, and API coordination.

Sri Lanka Telecom (SLT) also provides shared infrastructure services, and several solutions (such as the Suwapetha drug information system) are hosted on the SLT infrastructure. The security services domain describes a mechanism for node authentication which will permit the interchange of data in a secure manner between these two environments.

4.2.3.1 National Health Data Exchange (NHDX)

The National Health Data Exchange serves as the primary integration onramp into the DHP. The NHDX provides services related to:

- Message routing
- Mediation
- Validation
- Error logging & retry
- Service Discovery & Metadata Exchange
- Logging
- Load Balancing
- Publish & Subscription Management
- API Access Control

4.2.3.1.1 Messaging Services

The messaging services provided by the NHDX primarily are concerned with the receiving and sending of structured messages using standards-based interchanges from points of service to those other services within the DHP. The messaging services are responsible for:

- Exposing an API endpoint to points of service solutions,
- Transport of data between trading partners in the DHP,
- Encryption and decryption of message payloads as they are sent or received,
- Logging of messages received and sent (such as HTTP logs), and
- Terminating TLS connections.

The NHDX is required to support multiple messaging formats and standards including:

- HL7 Fast Health Interoperability Resources (FHIR)[30] for general purpose clinical data.
- HL7 Version 1 messages over secured Minimum Lower Layer Protocol (MLLP) where FHIR is prohibitive (such as integrating legacy or proprietary solutions)[31]
- IHE Aggregate Data Exchange (ADX) profile
- IHE Cross Community Document Sharing (XDS) using ebXML for sharing Radiology Reports, and other structured clinical documents[32]
- NEMA DICOMWeb[33] (which includes Web Access to DICOM Objects – WADO[34] and Query by ID for DICOM Object - QIDO[35]) for sharing PACS or RIS information to/from the DHP.
- GS1 Business Messaging Specification (BMS)[36] for logistics inventory reporting, and stock order request and fulfilment.
- Consistent time protocols using/exposing Network Time Protocol (NTP) to allow for enterprise synchronisation of time across the enterprise.
- IHE Audit Trail and Node Authentication (ATNA)
- OpenID Connect (OIDC)[37] and Open Authentication (OAUTH)[38] standards for authentication purposes.

[30] Http - FHIR v4.3.0 (hl7.org)
[31] mllp_transport_specification.PDF (hl7.org)
[32] Cross-Enterprise Document Sharing - IHE Wiki
[33] DICOMweb™ (dicomstandard.org)
[34] Retrieve (WADO-RS) (dicomstandard.org)
[35] Search (QIDO-RS) (dicomstandard.org)
[36] GS1 XML standards 3.5.1 - GS1 XML | GS1
[37] Final: OpenID Connect Core 1.0 incorporating errata set 1
[38] RFC 6749 - The OAuth 2.0 Authorization Framework (ietf.org)

Additionally, the NHDX should consider that this list will change over time as new technologies and methods of integrating health and supporting data arise. The NHDX should be implemented in such a way that other binary TCP protocols, HTTP based REST and SOAP protocols can easily be integrated.

4.2.3.1.2 Mediation Services

Mediation services of the NHDX include any steps which are required to ensure that message integration formats, patterns, and data are reconciled prior to message processing continuing within the DHP. Mediation services include:

- Filtering, removing, or appending appropriate message data to outbound messages,
- Queueing the message to ensure reliable delivery and allowing for retry of message errors,
- Caching, or storing messages to improve performance or ensuring execute once (i.e., prevent duplicate execution of triggers),
- Rewriting or augmenting URLs or pointers where appropriate for outbound data to ensure that points of service don't attempt query of back-end services.

4.2.3.1.3 Validation

The NHDX is responsible for the validation of messages which it receives. The validation of the message at the NHDX level focuses only on transport, structure, and terminology whenever a repository service cannot perform this validation. Examples of validation which can be performed at the NHDX level are:

- The message trigger event is appropriate, and a business process, destination repository, or service is known (message can be routed)
- The message structure is complete and matches the expected contents of the class of message (i.e., message header is present, message payload is present, digital signatures are present)
- Validation of digital signature of the submission of the message (i.e., the message has not been tampered with since it was sent)
- Validation of the syntax and structure of the message against schema or structure profile
- If the message contents are encrypted separate from transport layer (for example, using JSON Web Encryption, MIME Encoding, etc.) then the NHDX would be unable to validate the payload, however, can validate the wrappers for the content.

Clinical validation of the message contents (example: last menstrual period for a male) would be a large undertaking at the NHDX level, and instead these types of business rule validations should be performed by clinical expert systems (i.e., the NHDX should contact some expert system to validate the clinical content, or the repository servicing the data should perform the validation). The NHDX can perform such validation either by sending the transaction to the appropriate service, or by issuing a validation[39] operation where supported.

4.2.3.1.4 Error and Retry

The error handling and retry functionality of the NHDX is responsible for classifying and gathering error information relayed from the back-end repository service which produced the error, and relaying this to administrators.

Messages which resulted in an error within the NHDX will be queued for later administrative retry. For example, when a discharge summary is received by the NHDX and the NEHR record repository is offline, the NHDX should try to resubmit the message later.

[39] Operation-resource-validate - FHIR v4.3.0 (hl7.org)

Errors and inability to route, mediate, or interpret messages should be available to administrators of the NHDX to diagnose issues and perform corrective actions. Additionally, the NHDX should support administrative alerts on transactions that fail due to infrastructure issues (rather than clinical, or business issues).

4.2.3.1.5 Service Discovery & Metadata Exchange

Within a standardised, complex enterprise environment (which the DHP will represent), it is important that services and clients can understand where services are within the enterprise. The role of the service discovery and metadata exchange component is to facilitate:

- *Service Discovery:* Permitting clients / consumers of the component to obtain a list of services which are provided by the enterprise, and where these services are located.
- *Metadata Exchange:* Permitting clients/ consumers of the component to obtain a structured listing of the security policies, message formats, data requirements, etc.

Because the DHP represents a heterogenous environment with multiple standards, there are several proposed mechanisms which provide this functionality:

- HL7 FHIR Capability Statement,[40] Implementation Guide[41] and StructureDefinition[42] resources which describe a FHIR endpoints metadata, allows API operations, etc.
- OpenID Connect Discovery[43] which allows authentication clients to discover the policies (scopes), authorization endpoints and functions of the identity provider infrastructure in the DHP.
- OpenAPI[44] which allows any REST based API to expose metadata and discovery information in in a structured format

The blueprint proposes that the DHP infrastructure expose the details of service discovery and metadata exchange in the format most convenient, however, the DHP should expose all rest services metadata using OpenAPI[44]. For example, a FHIR REST service within the DHP will expose endpoint and security authorization information on the OpenAPI endpoint as well as relevant FHIR resources for conformance.

4.2.3.1.6 Logging

All DHP transactions must be logged and audited. The logging functionality in the NHDX describes the logging of access requests against the NHDX, and auditing of transactions is based on the requirements established in logical views and should be performed with the NHDX as the receiver and as the sender (i.e. receiver with the point of service, and sender with the backing service).

4.2.3.1.7 Load Balancing

Load balancing of transaction requests and throttling of messages coming from client systems is an important performance characteristic which must be provided by the NHDX.

Intelligent load balancing is a preferable future state, however the blueprint proposes simple DNS based load balancing such as round-robin. Additionally, the NHDX will also perform operations to ensure the safety of the DHP including:

- Service throttling and/or restriction when intensive messaging load is placed on the DHP,
- Ensuring the payloads submitted to the DHP via the NHDX are within an appropriate size limit,

[40] CapabilityStatement - FHIR v4.3.0 (hl7.org)
[41] ImplementationGuide - FHIR v4.3.0 (hl7.org)
[42] StructureDefinition - FHIR v4.3.0 (hl7.org)
[43] Final: OpenID Connect Discovery 1.0 incorporating errata set 1
[44] OpenAPI Specification v3.1.0 | Introduction, Definitions, & More

- Ensuring that when one node of a backing service within the DHP is down, the message is routed to another node which is available (i.e., failover)

The exact method of load balancing will depend on the specific architecture of the products used for implementation of the NHDX, which is out of scope of this blueprint document.

4.2.3.1.8 Publish and Subscribe

The NHDX implementation should seek to support a publish and subscribe (pub/sub) functionality. A publish and subscribe pattern allows applications to be subscribed to events which meet a certain criteria. When a trigger is executed which matches this subscription, the subscriber is notified with this information. For more information about this pattern in FHIR, the Subscription[45] resource may be consulted.

4.2.3.1.9 API Access Control

The NHDX will perform API access control. This control will be performed using the following techniques:

- The API access token in the content of HTTP messages will used to determine access control rules for the application, and in the future, users.
- Client certificates submitted with the request by the sending node to authenticate the node.

DHP components behind the NHDX will apply appropriate business logic checks and access controls based on the access token and any client assertions included on requests.

4.2.3.2 Terminology Services

PoS solutions across the country often use different, and custom terminologies (sometimes referred to as data dictionaries), to computationally describe health data. Records in one system may indicate the patient being administered “amoxicillin” using a custom code where another may indicate “amoxycillin” with a different code. Without common terminology, the semantic meaning of records may not be matched.

A terminology server assists in the harmonization of these terms by providing standardized code lists and services for the transformation of data.

The terminology services provided within the DHP represent a shared set of infrastructure services for the management, dissemination, validation, and coordination of terminologies in use within the DHP. Terminologies identified for use in Sri Lanka Digital Health systems include[46]:

- Systematized Nomenclature of Medicine Clinical Terms (SNOMED-CT) – Where possible, use of the Global Patient Set (GPS)[47] is encouraged.
- International Classification of Disease (ICD) Release 10[48] (ICD Release 11[49] is being investigated)
- Logical Observation Identifiers Names and Codes (LOINC)[50]

A terminology service allows for the management of these standardised codes by MOH administrative staff. The services for the terminology service can then be used by any service in the DHP to:

- Validate a concept’s use in a particular context is permitted (for example: restricting immunisation terminology codes to only those used in country)

[45] Subscription - FHIR v4.3.0 (hl7.org)
[46] National Digital Health Guidelines and Standards [2] Section 7.6
[47] SNOMED - Global Patient Set
[48] ICD-10 Version:2010 (who.int)
[49] ICD-11 (who.int)
[50] Download LOINC – LOINC

- Provide lookup of value sets for population of local code lists in software, or in user interfaces.
- Provide mapping functions for lookup of alternate codes in different code systems (for example: mapping an ICPC code to ICD)
- Provide workflow support for the review, approval, translation, and integration of new concepts into existing value sets.

4.2.3.3 Record Locator / Index

The record locator service provides indexing (or a table of contents) to health information within the DHP. This is useful since, as the DHP evolves, the index can provide:

- Linking between disease specific repositories of information within the DHP context
- Pointers to binary large objects (BLOBs) which cannot be submitted to a central DHP repository, but must be directly retrieved from source (such as CT or MRI image data from a RIS or digital pathology information)
- Linking between discrete data submissions (like FHIR or CDA resources) and binary document submissions (like images or PDFs)

The record locator saves the DHP from performing repeated queries against multiple repositories of information, permits federation of the repository information, and allows evolutionary growth (by adding additional repositories of information rather than upgrading one large repository “in place”).

The concept of a record locator mimics the functionality of a Document Registry in the IHE XDS profile[51] and should contain:

- The metadata / identification of the patient for which the information is linked,
- The location of the repository and specific data (registry identification / URL and data identification),
- Select metadata about the linked data such as timestamps, type of information (discharge, referral, transfer, etc.), and metadata which may be queried,
- The source of the information (facility, organisation, health worker, or patient), and
- A digital signature or checksum of the original data to allow for verification.

Early implementations of the blueprint where a single data repository is implemented (such as the NEHR Record Repository) can forego the implementation of a record locator – however as multiple repositories are implemented, the role of the locator becomes ever more important.

4.2.3.4 Business Process Execution

Business process execution function of the common infrastructure is responsible for the operationalisation of business workflows within the DHP enterprise. This is aligned with the orchestration services provided within an enterprise service bus which is used to:

- Coordinate service calls within the DHP which require multiple service calls,
- Execute conditional message passing based on programmed business rules,
- Perform compensation actions when service coordination fails.

The business process execution functionality within the common infrastructure could be used to execute clinical processes, however this represents a misuse of such a service a shared infrastructure context.

In keeping with the principle of loose coupling and service cohesion, clinical workflows, decision logic, or infrastructure processes (like de-duplication, matching, merging, etc.) are better left to specific expert systems or domain repositories since they are designed with specific business functionality in mind with guidance from experts in that domain.

[51] IHE ITI TF Vol1 Cross Enterprise Document Sharing

Additionally, attempting to coordinate a clinical flow across multiple repositories can introduce anti-patterns such as the need for distributed two-phased commits of information (example: POST to service A succeeds, but POST to service B fails, service A requires a "rollback").

Rather, the goal of common business process execution is to coordinate cross-service calls with atomic business operations. This may include steps to validate messages, cross reference data, and/or notify secondary repositories.

4.2.3.5 Common IT Infrastructure Services

Throughout the assessment phase of the digital health blueprint's development, there was a consistent identification of common features/ functions which points of service, and DHP services would need to leverage. Common IT infrastructure services of the DHP will service these needs in the future to reduce duplication of effort and cost, and should include:

- *Push Notification services* – providing secured APIs for issuing push notifications directly to applications in the MOH and secure instant messaging infrastructure.
- *SMS Gateways* – providing consistent integration point between digital health solutions and the SMS notification network. Common gateways would reduce cost in negotiating short codes with telecom providers, provide consistent APIs for digital health solutions for sending SMS notifications, and permit the consistent auditing and logging of communications sent to patients and providers.
- *Payment Services* – providing consistent payment services where digital health solutions require the processing of monetary transactions with banking or insurance payment infrastructure. Such use cases for this include co-pays, deductibles, cash payment for non-covered services or devices, payments for supplies, etc.
- *E-Mail Services* – the creation of an e-mail infrastructure for use within the health sector would provide a major improvement in the security and protection of official information used in the delivery of health care. Providing official e-mail addresses to staff, providers, officers, and administrators allows for monitoring of content sent for official purposes, allows the protection of information between mailboxes, and allows for allow-listing or block-listing for accounts and two-factor authentication. Additionally, setup of common e-mail infrastructure (a private SMTP and IMAP server) would allow digital health services to send e-mails to patients and providers from official MOH e-mail addresses.
- *Security Information Event Management (SIEM)* – infrastructure is used to monitor operating system and application events generated by DHP service infrastructure and is a common component used in many network operation centres. This infrastructure allows operations staff to monitor security events (such as invalid login attempts, repeated requests, or system faults) and quickly correct these.
- *Application Performance Management (APM)* – infrastructure is used to monitor the health and availability of virtualised infrastructure. APM solutions can often alert operations staff when service quality is degraded (response times, or compute resources are too high), or when components of DHP services are unresponsive (such as databases being in a degraded state, in recovery, etc.)

Several initiatives have already begun which should be reused and leveraged to fulfil these functional components, for example:

- ICTA provided GovSMS service fulfilling the role of SMS Gateway
- ICTA provided Lanka Government Payment Service (LGPS) or pay.gov.lk fulfilling the role of Payment Services

- LGN E-Mail or the (currently in development) Government Email Solution fulfilling the role of E-Mail Services
- ICTA provided LGC SOC (currently in development) fulfilling the role of SIEM monitor.

4.2.4 Health Administration

The conceptual components of the health administration domain are illustrated in Figure 18.

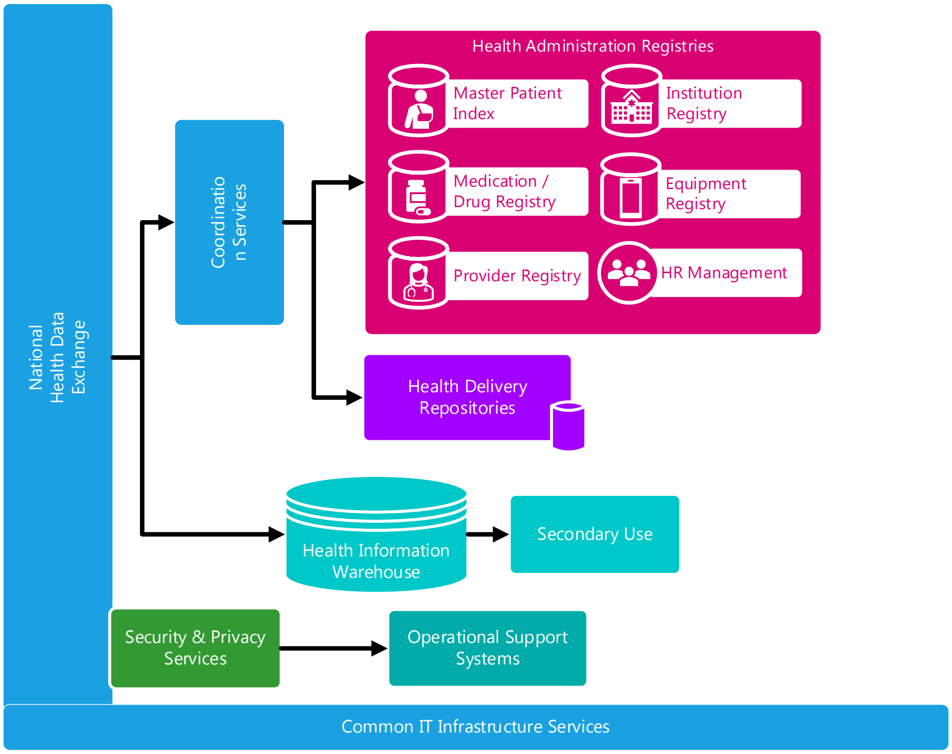

National Health Data Exchange
Coordination Services
Health Administration Registries
Master Patient Index
Institution Registry
Medication / Drug Registry
Equipment Registry
Provider Registry
HR Management
Health Delivery Repositories
Health Information Warehouse
Secondary Use
Security & Privacy Services
Operational Support Systems
Common IT Infrastructure Services

Figure 18 : *Health Administration Conceptual Components*

The health administration domain is primarily concerned with the identification of resources which are used in the support of delivery of health care. This domain encompasses:

- Identification of Patients/Clients
- Identification of Health Workers
- Identification of Institutions
- Identification of Medications and Implantable Medical Devices
- Human Resources Management
- Logistics Support

4.2.4.1 Client Registry

The DHP represents a patient centric enterprise architecture which is responsible for the integration of health data across disparate health solutions. Patient centric means that the DHP must track the identification of recipients of care (both Sri Lankan citizens and non-citizens such as foreign dignitaries, workers, and medical tourists). To ensure that the correct data is assigned and linked to the correct recipient of care, it is important that the DHP have a known registry of all recipients of care for which health information is being captured.

The role of a client registry within a healthcare enterprise is well defined[52,53] , at a high level the client registry in Sri Lanka is expected to:

[52] IHE.ITI.PMIR\1:49 Patient Master Identity Registry (PMIR) Profile - FHIR v4.0.1

[53] Client Registry (CR) - OpenHIE Architecture Specification (ohie.org)

Accept registrations of new patient information records (citizens or visitors)

- Manage the registration of patients within the digital health enterprise (i.e., death, change of residence, updates to demographics)
- Provide identification cross referencing to/from a consistent enterprise identifier
- Provide restricted demographics query functionality (see description below)
- Provide linking, merging and un-merging functionalities as duplicate registrations are detected and reconciled

The MPI should implement the minimum dataset[54] and be capable of cross-referencing the following identifiers to an enterprise unique identifier:

- Citizen Identification Number
- Sri Lanka Identification Number (SLIN)
- Personal Health Number (PHN)
- Passport Number (for foreigners)

Because the client registry contains sensitive demographics and identity for patients, queries should be restricted in the following manners:

- Enforce minimum number of search parameters (i.e., must query by Name + Gender + District or PHN + Gender), and
- Enforce a maximum number of search results (i.e., maximum of 20 results), and
- Disallow general “wildcard” searches or bulk queries/synchronisation.

4.2.4.2 Provider Registry

The distribution of health records across organisations and services necessitates the consistent identification authorized person to carry out specific task according to a specific legal act. which are responsible for the delivery of care services. This is the primary role of the provider registry (sometimes called as health provider directory, or health worker registry). Additionally, many health provider registries offer linkage to provider’s service delivery capabilities (i.e., dermatology, oncology, or others) which can be used for matching providers with patients in need of those capabilities, specific specialist medical care.

The primary responsibility of a provider registry is well defined[55],[56] and can generally be summarised as:

- Accepting official registrations and updates from official sources like the Sri Lanka Medical Council (SLMC) and Sri Lanka Nursing Council (SLNC) who enlist the individual names who can carry out specific health are delivery process..
- Providing a linkage between providers and the roles that provider plays (i.e., primary care physician, oncologist, tertiary care facility, immunisation clinic, or others)
- Cross referencing of provider identifiers to an enterprise identifier for each provider.
- Providing queries for PoS to understand the active status of the provider (i.e. revocation of license to practice).
- Discovery of health providers (persons or organisations) based on their registration details (such as address, telephone, name, or services).

The provider registry in the DHP should implement the minimum dataset[57] for providers, and should be capable of cross referencing the following identifiers with an enterprise unique identifier with:

[54] National Digital Health Guidelines and Standards [2] Section 7.4
[55] IHE Health Provider Directory Supplement
[56] National Digital Health Guidelines and Standards [2] Section 7.3
[57] National Digital Health Guidelines and Standards [2] Section 7.4

- Professional Registration Number and Issuer
- National Identification Number (NIC)
- Sri Lanka Identification Number (SLIN)
- Other individual provider identification numbers, for example:
    a. Private Health Services Regulatory Council number
    b. Passport Number (for foreign or visiting providers)

4.2.4.3 Institution Registry

The health institution registry is responsible for the maintenance of a country-wide manifest of public and private facilities for which data may be registered in the DHP. The role of an institution or facility registry is well defined in other standards[59], and can be summarised as:

- Collect, store, and disseminate an authoritative master facility lists (MFL)
- Provide classification and registration of services offered in each facility to allow for service discovery,
- Cross reference facility registration records and identification from disparate sources such as the Ministry of Health (including national, apex, base, teaching, primary care and specialist hospitals) and the Private Health Sector Regulatory Commission (PHSRC),
- Provide query capabilities allowing other digital health services to locate service delivery locations based on their attributes.

The institution registry in the DHP should implement the minimum dataset specified for Sri Lanka[60] and should provide functionality for cross referencing local identifier for facilities (obtained from source registration systems for facilities) with a unique enterprise identifier.

4.2.4.4 Medication & Device Registry

The registration of a central drug registry is of high importance for providing a definitive list of reference medications and devices which may be referenced within the NEHR or procedure records.

A medications and device registry will be used to track the substances (supplements, vaccines, therapeutics, or other) and medical devices (pacemakers, prosthetics, insulin pumps, etc.) which can be ordered, delivered, prescribed, and administered within the country.

The primary functions of such a drug registry are:

- Provide consistent identification of drugs and materials beyond simple codes (which merely classify a type of drug, rather than a particular product)
- Provide classification of medications using standardized codes (WHO ATC[61], SNOMED CT[62], CVX[63], RxNORM[64])
- Provide detailed information about the form, ingredients, and size/quantity of the medication,
- Provide linkages with types of registered drugs with manufactured products which can be ordered and tracked through cross-organisation logistics workflows,
- Allow for rapid withdrawal of products and lot numbers based on manufacturer guidance.

[58] Evaluation of Electronic Health Information Systems (HIS) for the Ministry of Health, Nutrition, and Indigenous Medicine [5] Table 6 - https://arch-lk.health/dmsf/files/3/view
[59] OpenHIE Facility Registry Implementation Guide - Google Docs
[60] National Digital Health Guidelines and Standards [2] Section 7.3
[61] Anatomical Therapeutic Chemical (ATC) Classification (who.int)
[62] Drug or medicament (snomedbrowser.com)
[63] IIS | Code Sets | CVX | Vaccines | CDC
[64] RxNorm (nih.gov)

The implementation of the medications and drug repository will implement appropriate HL7 FHIR[65] resources as a baseline, and should include support for appropriate logistics support messages such as GS1 BMS Product Recall[66] and Item Data[67] transactions.

4.2.4.5 Equipment & Supplies Registry

The ordering and reporting of non-substance supplies (such as syringes, scalpels, bandages, etc.) within the DHP necessitates the implementation of a supplies registry to track inventory, ordering and delivery, and withdrawal of supplies.

The primary functions of the equipment registry are:

- Collect, store, disseminate registration information of new consumables and equipment stock items which are approved for use in Sri Lanka.
- Provide query and lookup for services within the DHP allowing those services to link data within logistics inventory reports, facility assignments, and stock orders/despatches/arrivals to registered equipment.
- Provide a master list of device regulatory information including status (pending, active, withdrawal, etc.), manufacturers, and suppliers.

The implementation of the equipment and supplies repository will implement appropriate HL7 FHIR[68] resources, and may support messages such as GS1 BMS Product Recall[66] and Item Data[67] transactions.

4.2.5 Health Delivery

The primary purpose of the DHP services contained within the health delivery business domain services the needs of managing information and processes which facilitate the delivery of care. Examples of data and services within the delivery of health care are:

- Admissions and discharges to/from hospitals within Sri Lanka
- Referrals to specialised care providers, or transfers between hospitals
- Diagnoses and treatment of non-communicable and communicable diseases
- Pharmaceutical workflow coordination (prescription, foundry, dispense, administration and status)
- Chronic disease management and coordination
- Immunisation and prophylaxis information
- Transplant wait-listing and donor matching processes
- Laboratory procedure orders, specimen collection and tracking, and result reporting
- Diagnostic Imaging orders, imaging results, and diagnostic reports
- Nutrition and dietary management, planning and follow-up
- Patient summaries representing the current health status of the patient (family history, social health status, behavioural analysis, etc.)
- Public health and health promotion
- Disease surveillance, quarantine monitoring and contact tracing
- Conditions, health problems and concerns
- Allergies, intolerances, and adverse events
- Vital signs observations (weight, height, conditions)

The components within this domain are illustrated in Figure 19.

[65] Medication - FHIR v4.3.0 (hl7.org)
[66] Product Recall | GS1
[67] Item Data Notification | GS1
[68] Device - FHIR v4.3.0 (hl7.org)

These concerns are managed within the health delivery subject area, which provides:

- *Shared Data Repositories:* Which are used to store structured, clinical information about the patient including the NEHR Record Repository, Imaging Repositories, Disease and Domain repositories. These repositories require the use of heterogenous data formats based on their domain, so the DHP defines a pattern of multiple repositories (like PDFs, DICOM WSI images, digital pathology systems, and genomics) to facilitate this requirement.

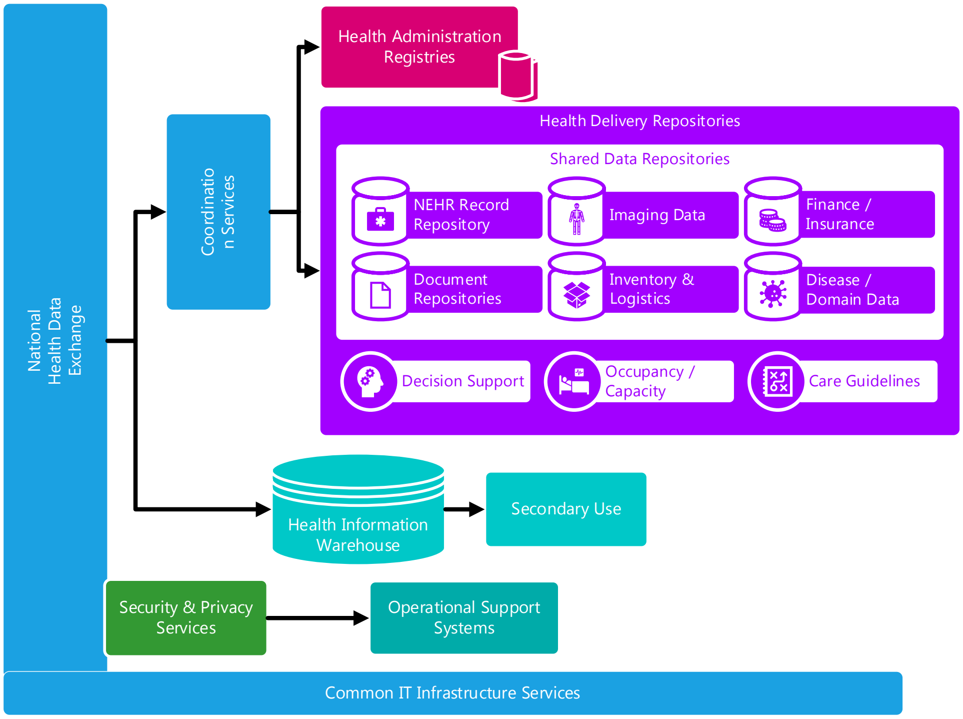


Figure 19 : *Health Delivery Domain Conceptual Components*

- *Decision Support Services:* Which are used to provide clinical decision support to systems by proposing actions which should occur in order to adhere to a best practices, or relevant clinical protocols.
- *Care Guideline Repositories / Clinical Knowledgebases:* For storing the definition of clinical protocols in machine readable and human readable forms.
- *Inventory and Logistics Services:* The digital capturing, management, and reporting of stock levels, ordering and despatching stock.

4.2.5.1 National Electronic Health Record (NEHR) Repository

The minimum dataset for a standing, shared patient summary was defined in the NDHGS[69]. The goal of the NEHR Record Repository is to provide the necessary storage and retrieval capabilities for these data summaries.

The format and content and transaction profiles for the NEHR Repository will require extremely detailed documentation, and these will be contained in NEHR interoperability profiles and logical design.

[69] National Digital Health Guidelines and Standards guide [2] section 7.7

At a high-level, the role of the NEHR is:

- Facilitate the storage and amendment of a shared patient's summary record whenever the patient is admitted to outpatient, special clinicals, public health settings, specialist setting or other settings.
- Facilitate the query of the patient's shared summary information from the NEHR repository on demand of a consuming application.
- Adhere to, and protect, data disclosures using the security tags which have been applied to the data records.

The NEHR Repository will act as the foundational piece of a shared health record for the patient, providing patient medical summaries in a standardised format. The information flows and types of data which are stored in the NEHR Repository are outlined in section 5.2.3 on page 108. The preferred method of representing data within the NEHR is HL7 FHIR R4, the details of which will be produced in technical views (implementation guides).

4.2.5.2 Imaging Repositories

The shared imaging repositories within the DHP are designed to store and disseminate the result of diagnostic imaging studies performed within Sri Lanka such as radiology, pathology, and ophthalmology.

The DHP proposes alignment with the pattern defined in the IHE Cross Enterprise Document Sharing for Imaging (XDS-I)[70] and the RESTful Web-Based Imaging Access (WIA)[71] profile. In this pattern, imaging reports and manifests are shared via the NHDX to the imaging repositories in the enterprise. These manifests are registered in the record locator with select metadata (such as provider, organisation, patient identity, type of study, title, etc.) where compatible points of service (such as EMRs, PHRs, viewers, etc.) then query for and retrieve manifests and radiology reports and point to the diagnostic imaging repositories (DIR) where the images reside.

Additional details about the DIR design should be developed as part of the diagnostic imaging logical design view and interoperability profile. Figure 20 provides an illustration of the IHE XDS-I profile with a mapping to services/components within the DHP for context of the reader.

4.2.5.3 Disease & Program Specific Repositories

The evolutionary nature of the blueprint and DHP it proposes means that new features and areas of concern must be integrated into the architecture without disruption or change to existing solutions. The DHP proposes disease specific repositories of information to be created in addition to the NEHR repository. The rationale for this is:

- Isolation of software solutions to fit the clinical use case (best tool for the job),
- Isolation of standards based on their maturity and suitability for a particular purpose,
- Existing software in use in Sri Lanka already implemented along disease and programs,
- Specialised validation logic for a particular disease or program can be separated in smaller solutions instead of a large monolithic solution,
- Differing scopes of data can be facilitated – for example, the storage of individual child health records by the Family Health Bureau may contain information which is important for child care beyond the scope of the NEHR.

[70] Cross-enterprise Document Sharing for Imaging - IHE Wiki

[71] Web-based Image Access - IHE Wiki

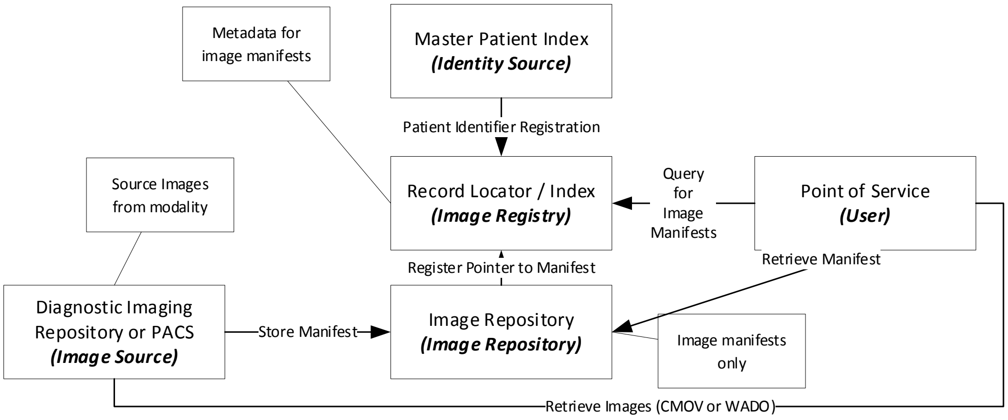

Metadata for image manifests
Master Patient Index
(Identity Source)
Patient Identifier Registration
Source Images from modality
Record Locator / Index
(Image Registry)
Query for Image Manifests
Point of Service
(User)
Register Pointer to Manifest
Retrieve Manifest
Diagnostic Imaging Repository or PACS
(Image Source)
Store Manifest
Image Repository
(Image Repository)
Image manifests only
Retrieve Images (CMOV or WADO)

Figure 20 : *XDS-I Image Exchange in DHP*

The DHP proposes using a registry of records (the record locator) with metadata and pointers to the various repositories of information (NEHR Repository, Domain Repositories, etc.). This pattern mimics the IHE XDS[72] architecture and allows for a single table of contents to reference multiple repositories which are more well suited for their domain of expertise.

4.2.5.4 Clinical Document Repositories

The role of documents within a health enterprise is important as they provide wholistic, validated, and complete representations of an event as the originating provider documented it. Clinical documents are a useful documentation pattern for:

- Summarising encounters or visits by an institution (examples: discharge summaries, visit summaries)
- Summarising or providing rationale for a diagnosis or condition (example: diagnostic note)
- Summarising information between modalities (example: radiology report based on ultrasound capture)
- Representing signed, stand-alone medically legal documentation from a provider which cannot be altered, transformed, or changed (although, derivative information can be extracted, the original document cannot be changed)

In electronic health records systems, documents are prepared from discrete health events within the point of service system, then validated by the provider, optionally digitally signed, and submitted as a single, in-context submission to the shared infrastructure.

HL7 CDA (Clinical Document Architecture) defines three types or levels of codification for clinical documents[73]:

- *Level 1* – Metadata about the document is codified such as patient identity, provider identity, classification of the document (discharge, referral, radiology report, etc.) a title and other metadata. The content of the document, however, is binary.
- *Level 2* – The metadata from level 1 is codified, and structured information about the sections of the document are also present (discharge medications, vital signs, problems/conditions, primary concern, etc.) however the content of the sections can be un-structured.

[72] IHE ITI TF XDS.b Vol1
[73] HL7 CDA | Lyniate

- *Level 3* – The entirety of the document structure is encoded such that discrete data elements can be computationally read and semantically interpreted.

HL7 FHIR provides a modernisation of CDA[74] via the Document resource, which is proposed as the primary method of submitting documents to the DHP.

Because of the usefulness of clinical documents, and their ability to represent original summaries of clinical events, the DHP proposes the implementation of clinical document repositories which can be used to store these structures.

The IHE Mobile access to Health Documents (MHD)[75] and Mobile Health Document Sharing (MHDS)[76] profiles provide a useful pattern for storing this information within the DHP. Figure 21 shows how the MHDS and MHD profiles from IHE logically map onto business services within the DHP.

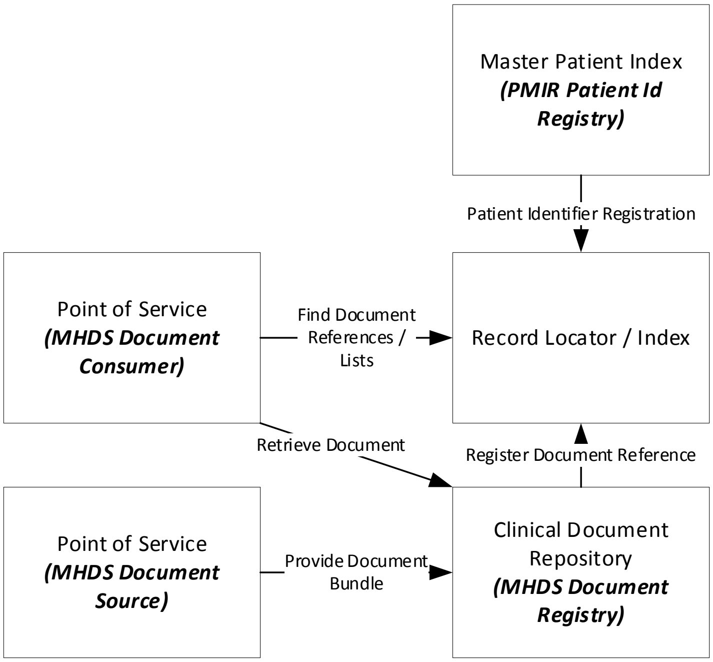

Master Patient Index
(PMIR Patient Id Registry)
Patient Identifier Registration
Point of Service
(MHDS Document Consumer)
Find Document References / Lists
Record Locator / Index
Retrieve Document
Register Document Reference
Point of Service
(MHDS Document Source)
Provide Document Bundle
Clinical Document Repository
(MHDS Document Registry)

Figure 21 : *MHD and MHDS in the DHP*

4.2.5.5 Inventory and Logistics Data

The ability to deliver health care within a care setting depends heavily on the availability of supplies for medication, surgical equipment, syringes, and more. Understanding stock usage patterns between organisations, and facilitation of electronic ordering within a standardised pattern of exchange is a useful function of a health enterprise.

The inventory and logistics data services of the DHP are responsible for:

- Collecting, managing, or producing inventory reports for service delivery points throughout Sri Lanka including reporting of stock-outs (where care could not be delivered due to lack of supplies).
- Facilitating solicited (order) and un-solicited (despatch without order) supply of equipment, materials, drugs, and devices to service delivery points.

[74] Documents - FHIR v4.3.0 (hl7.org)
[75] IHE.ITI.MHD\MHD Home - FHIR v4.0.1
[76] IHE.ITI.MHDS\1:50. MHDS Volume 1 - FHIR v4.0.1

- Collecting information about breakages, loss, and wastage of supplies to optimise use and reduce direct cost of replacement.
- Improving the stock management and distribution of materials within Sri Lanka for health settings – allowing for predictive stock management (preventing stockout situations).

There are HL7 FHIR resources for logistics, however the GS1 business messaging specifications (BMS)[77] represent a more widely adopted and mature series of interchanges for logistics and should be implemented as part of logistics and inventory processes in future.

4.2.5.6 Care Guidelines Repository

The care guidelines repository is intended to represent a storage solution of consistent care guidelines and clinical protocols for use within Sri Lanka. The DHP considers both non-computable care guidelines (PDFs of clinical assessment tools, procedures, etc.) and computable care guidelines (CCG)[78].

Evolutionary development of the care guidelines repository should consider the implementation of sharing for non-computable care guidelines using appropriate resources (such as FHIR documents or a knowledgebase system), and future development of CCG capabilities when sufficient maturity of the DHP is attained.

The implementation of CCGs such as WHO's SMART Guidelines[79] should be facilitated by distributing L2 (human readable) guidelines using the non-computable methods and L3 (machine readable) artifacts using FHIR Libraries[80].

The contents of this repository will include:

- Implementation guides which contain the overall narrative and technical descriptions of the standardised guidelines for Sri Lanka
- Definitions and conformance statements for the structure of data which needs to be captured from points of service.
- Libraries[80] of clinical decision support rules which can be executed by DHP services or points of service at the point of care.
- Standardised performance indicators which can be used by the DHIW and KPI repository to disseminate the measures which implementations are expected to report or trace.

4.2.5.7 Clinical Decision Support Services (CDSS)

The storage of care guidelines within the care guideline repository is a first step to the tracking of intelligent health systems. While robust points of service implementations can be expected to directly consume and execute/adhere to these care guidelines, the blueprint proposes the DHP expose necessary services for execution of CDSS rules by all services within the DHP.

The clinical decision support services exposed by the DHP should operate as a type of CDS-as-a-service pattern, which is defined in the CDS Hooks[81] architecture.

4.2.6 Secondary Use

The secondary use domain encapsulates all functionality which uses clinical data for purposes other than delivery of care. The electronic Indoor Morbidity and Mortality Register (eIMMR) is a

[77] GS1 set of XML standards | GS1
[78] Computable Care Guidelines - IHE Wiki
[79] SMART Guidelines (who.int)
[80] Library - FHIR v4.3.0 (hl7.org)
[81] CDS Hooks (cds-hooks.org)

primary example of a secondary use service currently leveraged within Sri Lanka, however other secondary use solutions exist for programmatic and monitoring purposes. These should be harmonised to provide a consistent implementation within the DHP.

- Geographic Information Systems (GIS) use cases for plotting coverages, wait times, service availability.

The conceptual services which compose the secondary use domain, and sample use cases of secondary use data are illustrated in Figure 22.

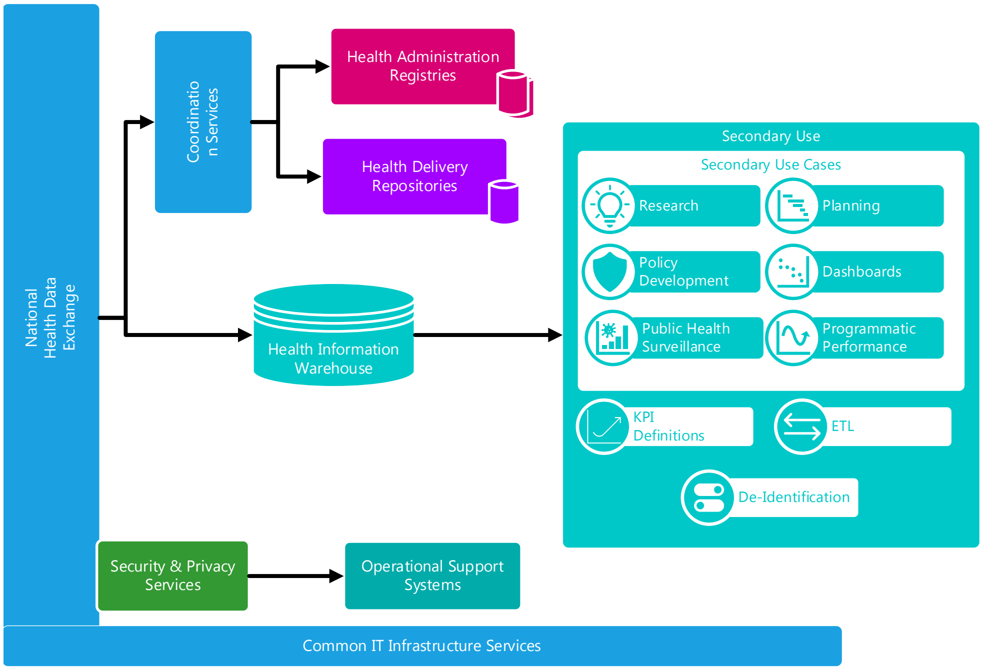

National Health Data Exchange
Coordination Services
Health Administration Registries
Health Delivery Repositories
Health Information Warehouse
Secondary Use
Secondary Use Cases
Research
Planning
Policy Development
Dashboards
Public Health Surveillance
Programmatic Performance
KPI Definitions
ETL
De-Identification
Security & Privacy Services
Operational Support Systems
Common IT Infrastructure Services

Figure 22 : *Secondary Use Domain Conceptual Architecture*

The primary purpose of secondary use components:

- Capture and definition of key performance indicators (KPI) for health systems monitoring and evaluation,
- Use of pseudonymised or anonymised discrete records data for clinical research, measuring the efficacy of novel interventions, contact tracing, or other use cases,
- Public health monitoring such as outbreak detection, defaulter tracing, dropout tracking,
- Drug and device recalls, tracking where a particular drug or device has been used and needs to be recalled and/or replaced,

Secondary use data will be collected in a variety of ways to populate the DHIW, some of which mimic patterns of use in Sri Lanka today, these include:

- Extraction of data from shared registries and repositories via an ETL process (extract, transform and load) whereby historical events for a reporting period are queried after recordation and the DHIW populated. This pattern is useful for trailing indicators or population of new KPI from historical data.
- Automatic reporting and calculation of secondary use data directly from points of service, registries or repositories using definitions managed by the secondary use system. This pattern is like an ETL process,

except each software system computes the data from its own data store and prepares a summary report to the DHIW.

- Automatic capture of secondary use data via the national health data exchange based on subscriptions the DHIW has with the NHDX.
- Manual electronic capture of secondary use data via questionnaires which are populated by administrative users. This pattern is useful for administrative or non-clinical use cases such as functional status of equipment, planned outreach sessions, and others.

4,2,6,1 Digital Health Information Warehouse (DHIW)

Existing systems serve the role of secondary use repository including the eIMMR, and programmatic monitoring data via various DHIS2 implementations. The blueprint proposes the establishment of a unified digital health information warehouse, responsible for the storage and tracing of health data events within the DHP.

The responsibilities of the DHIW include:

- Storage of measure values[82] and health system status questionnaire responses[83] submitted to the DHIW service via the NHDX
- Population of data directly from NHDX subscriptions as data flows through the enterprise
- Receipt of aggregate data exchange (ADX) measurements from databases.
- Disclosure of indicator measure values via APIs (ADX, or HL7 FHIR Measure Reports[82]) which can be used by authorised third-party sources.

There are several proposed methods of the capture data and population of the DHIW in future state of the DHP, some of which mimic current data capture methods used in Sri Lanka. These information flows are documented in section 5.2.4, on page 109.

The physical design of the DHIW is out of scope of the blueprint, however a variety of strategies will be employed depending on the use case of the data marts such as:

- Traditional RDBMS (Relational Database Management System) warehouse schema with defined data marts using a standardised practice such as Data vault[84] modelling.
- OLAP (Online Analytical Processing) cubes
- HL7 FHIR MeasureReport and Questionnaire response storage and retrieval
- An implementation of the District Health Information System Version 2 (DHIS2) software

4.2.6.1.1 Extract Transform Load (ETL) Services

While the distribution of computable KPI to be completed by software solutions is possible, it is understood that not all software may be capable of performing these tasks. For this reason, the blueprint includes a provision for use of extract, transform and load (ETL) [85] services.

ETL jobs are defined by data analyst teams and written in software which supports the bulk loading and transformation of data from source systems using either database extraction, or SOAP / REST API extraction. The process then performs calculations and transformations (such as pivoting, aggregating, etc.) and loads the result into the target database via database calls or API calls.

[82] MeasureReport - FHIR v4.3.0 (hl7.org)
[83] QuestionnaireResponse - FHIR v4.3.0 (hl7.org)
[84] Data vault modeling - Wikipedia
[85] Extract, transform, load - Wikipedia

4.2.6.1.2 KPI Definitions Repository

The blueprint proposes the implementation of a repository which can be used to allow the central line ministry of health to define indicators for which they would like PoS or the DHP infrastructure to capture.

These definitions should be managed and maintained by a KPI definitional repository which is used to express the standardised computation of these indicators from software in use in Sri Lanka. The form of these definitions could be:

- Narrative form such as a Wiki or PDF,
- Executable form such as Clinical Quality Language (CQL)[86] or Structured Query Language (SQL)[87]
- As FHIR definitions such as:
  a. Measure[88] - for data which can be computed directly from FHIR resources
  b. Questionnaires[89] - for data which cannot be computed but must be captured on a regular cadence (example: regular reporting of cold storage functionality)

The definition of these artefacts can be downloaded by the capable points of service, registries, and repositories to produce necessary measures to the health information warehouse.

4.2.6.1.3 Data De-Identification

Whenever a third party requires individually identifiable data for programme objectives, a process of de-identification should be performed.

The de-identification service within the secondary use domain will provide services for the appropriate de-identification of data based on requirements of how the data will be used. ISO/TS Standard 25237[90] describes the objectives of de-identification, and includes:

- Secondary use of clinical data (e.g., research).
- Clinical trials and post-marketing surveillance.
- Pseudonymous care.
- Patient identification systems.
- Public health monitoring and assessment.
- Confidential patient-safety reporting (e.g., adverse drug effects).
- Comparative quality indicator reporting.
- Peer review.
- Consumer groups.
- Medical device calibration or maintenance.

The information flow and process for de-identification is described in further detail in section 5.2.6.3.1 on page 116.

4.2.7 Security & Privacy

Security and privacy concerns are a cross cutting functionality of all services within the blueprint and its ultimate implementation in the DHP. In the modern world, network and software vulnerabilities mean that services and points of service cannot simply rely on the DHP and NHDX security, and each service is expected to adhere to relevant technical principles related to privacy and security (see Functional Principles of).

The shared services related to privacy and security are illustrated in the context of the broader digital health platform in Figure 23.

[86] Clinical Quality Language (CQL) (hl7.org)
[87] sql1999.pdf (pdx.edu)
[88] Measure - FHIR v4.3.0 (hl7.org)
[89] Questionnaire - FHIR v4.3.0 (hl7.org)
[90] https://www.iso.org/standard/63553.html

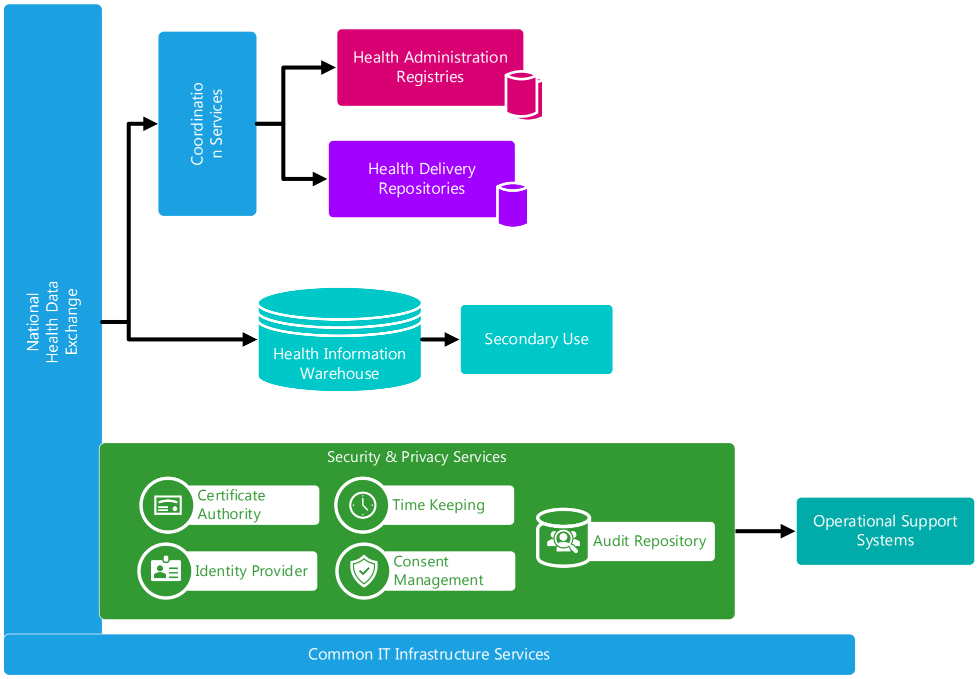

National Health Data Exchange
Coordination Services
Health Administration Registries
Health Delivery Repositories
Health Information Warehouse
Secondary Use
Security & Privacy Services
Certificate Authority
Time Keeping
Identity Provider
Consent Management
Audit Repository
Operational Support Systems
Common IT Infrastructure Services

Figure 23 : *Security & Privacy Domain Conceptual Architecture*

The primary concerns of the privacy and security components of the DHP are:

- Certificate Management used as the basis for cryptographic digital signatures, node authentication, and encryption of data.
- Authentication Services to ensure application and (in the future) identity and access control of DHP resources.
- Consent Services used to track the opt-in or opt-out of patients and enforcement of tagged policies.
- Common Auditing services, vital to ensure appropriate access to health data, investigating misuse, and providing patient's summaries of who is accessing their data.
- Consistent timestamping services

4.2.7.1 Time Keeping / Consistent Time

When integrating health data and security events between nodes on different infrastructure hardware, and between organisations, it is of vital importance that a consistent "official" time be kept within the enterprise.

The DHP proposes either the implementation of a time server, or the adoption of a consistent third-party time server (such as time.windows.com). This service should adhere to the Network Time Protocol (IETF RFC1305)[91] and the considerations for an enterprise timekeeper is described in IHE Technical Framework[92].

4.2.7.2 Certificate Services

The principles and design of the blueprint relies on cryptography to protection of data at rest, in transit and for digital signatures (establishing trust of data). The DHP should provide services related to functions which support this including:

- A Certificate Authority (CA) which is responsible for issuing, revoking, generating, and managing encryption certificates using RSA public/private key architecture[93]

[91] RFC 1305 - Network Time Protocol (Version 3) Specification, Implementation and Analysis (ietf.org)
[92] IHE ITI TF Vol1 - Consistent Time
[93] RFC 3447 - Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 (ietf.org)

- A key distribution service (KDS) which allows services to obtain public keys for validation of signed data following the JSON Web Key[94] specification. The key distribution service should be publicly available and should use the JSON Web Key Set[95] pattern.

4.2.7.2.1 Security Certificates

Creating or adopting an existing certificate authority is a relatively straightforward and provides benefits such as:

- Authentication of device nodes[96] can be handled via TLS which provides a robust mechanism for blocking access to the DHP services to unauthorised nodes (or devices which lack an appropriate certificate).
- The MOH can issue, and revoke encryption certificates used for data transmission and storage.
- Intermediate certificate authority can be used to delegate the issuance and revocation of certificates.
- Trust for digital identity can be established via the certificate chain.
- Digitally signed data can be trusted (or not trusted) based on the issuer of the certificate used to sign data (example: digital health card signatures[97]).

The chain of trust for the DHP can be based and delegated based on provincial and central areas of concern as illustrated in Figure 24.

4.2.7.3 Audit Repository

That NDHGS defines the need for all digital health solutions to maintain an audit log of all creation, read, update, and deletion of health information[98]. The blueprint strongly proposes the DHP provide a centralised audit record repository at the earliest possible stage of the DHP development.

Audit repositories are vital within a health system as they provide a complete list of logical security and data events which occur within the enterprise and allow for investigation and tracking of user activity for compliance and patient privacy audits.

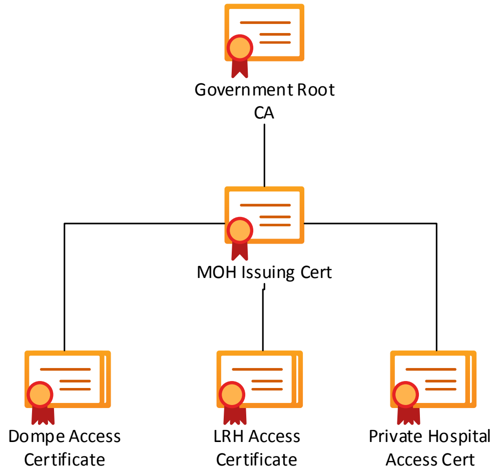


Figure 24 : *Certificate Chain of Trust*

[94] RFC 7517 - JSON Web Key (JWK) (ietf.org)
[95] JSON Web Key Sets (auth0.com)
[96] IHE ITI TF Vol2 – Authenticate Node
[97] SMART Health Cards Framework
[98] National Digital Health Guidelines and Standards [2] 6.3.3

A well-supported audit repository within the DHP allows administrators to:

- Produce privacy accounting and disclosure reports which indicate to whom and when data was disclosed.
- Provide privacy access logs which indicate what user accessed which data and why.
- Inspect daily activity for unusual events such as too many login failures by a user, requests for data from unusual places, etc.
- Prove that the users are following policy to access only appropriate data.
- Perform investigations on inappropriate accesses.

Audits differ from application logs in that an audit is not merely a free-text stream of application or systems events, rather they represent structured and curated notifications of events which impact the security, privacy, and data integrity of the DHP. The goal of the security audit repository is to answer:

- What event occurred?
- When did the event occur?
- Who (what people, organisations, users, devices, applications, etc.) was responsible for the event?
- Which resources were impacted by the event?

Points of Service within the DHP are required to keep localised audit trails within their own system software and should provide standardized APIs for query of those audits when requested.

Additionally, events in all interoperability profiles will indicate when PoS systems are required to send client side-audits to the central DHP audit repository. Certain classes of events will require order to aide in inappropriate access detection. These may include access to auditing failed searches, events where a security or consent block was triggered, etc.

The IHE ATNA (Audit Trail and Node Authentication) profile provides detailed documentation of the role and use of an enterprise audit repository within a health enterprise[99] and the blueprint recommends implementation of an audit repository which supports one or more of the following interchange standards:

- IETF RFC3881 over SYSLOG (UDP or TCP)[100]
- NEMA DICOM Audits[101]
- HL7 FHIR AuditEvent[102] resources (preferably using a standardised profile such as the RESTful ATNA profile from IHE[103])

The logical information model of the structure and contents of audits is discussed in further detail in section 5.2.4 on page 109.

4.2.7.4 Identity Provider

The digital health platform uses a services-oriented architecture whereby requests will be transmitted between software solutions via API service calls. This requires that each API know the identity of the calling application to apply specialised business rules, access controls, or privacy controls.

The DHP will use a bearer token strategy to facilitate the transmission of authentication context between services. The bearer token will be generated and digitally signed (to prevent tampering) from a centralised identity provider using the credentials issued to the PoS using OpenID Connect[104] and OAUTH 2.0[105]. This implementation should be

[99] IHE ITI TF Audit Trail and Node Authentication - Vol1
[100] RFC 3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications
[101] A.5 Audit Trail Message Format Profile (nema.org)
[102] AuditEvent - FHIR v4.3.0 (hl7.org)
[103] IHE_ITI_Suppl_RESTful-ATNA
[104] Specifications | OpenID
[105] Map of OAuth 2.0 Specs - OAuth 2.0 Simplified

compatible with SMART on FHIR[106] and IHE Internet User Authorization (IUA)[107].

The DHP will initially use a web of trust pattern for user authentication to reduce the complexity of deploying a centralised enterprise single-sign-on infrastructure. In this model, the presence of an application key, and node authentication certificate will only be issued to PoS solutions which have been validated to properly authenticate user credentials. A signed user assertion will be provided by PoS solutions until enterprise SSO can be established for the DHP.

4.2.7.4.1 *Application Authentication*

The issuance and revocation of API keys individually on each solution with the DHP would be time consuming, a prone to issues (revoking access requires that all access is revoked). The identity provider is proposed by the blueprint to be the central manager of application identity and API keys. The revocation of an API key on the identity provider would also result in immediate revocation to all services in the DHP. This flow is illustrated in Figure 25.

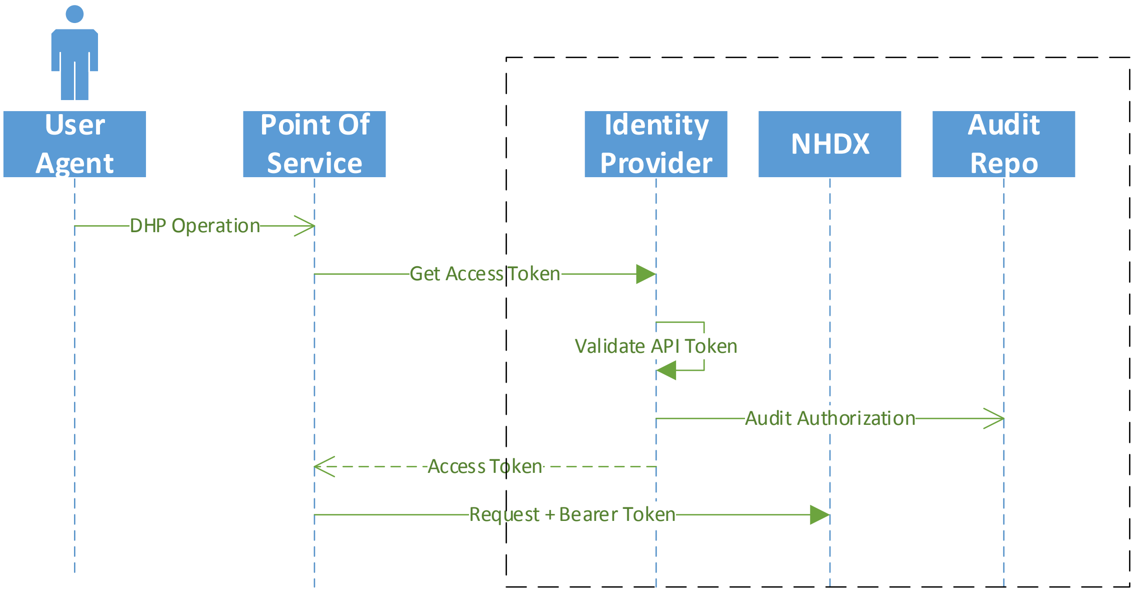


Figure 25 : *Client Credentials Flow*

4.2.8 Operational Support

Operational support systems are vital pieces of an enterprise as they assist in the effective management and use of personnel resources within the MOH. The operational support services identified within the DHP describe services which the MOH and ICTA provide which are not directly related to the sharing of health information. These services, however which can leverage the shared security infrastructure.

The operational support concerns include:

- Learning Management Systems (LMS) which to provide e-Learning courses to staff, providers, administrators, and other users of the DHP. As the DHP functionality grows, new policies are enacted, or general business processes, and new technologies invented the change management will be an important factor facilitated by the LMS.

[106] HL7.FHIR.UV.SMART-APP-LAUNCH\Overview - FHIR v4.0.1

[107] IUA (ihe.net)

- Helpdesk(s) and issue ticketing systems are a key piece of any operational enterprise software solution. It is important to ensure that operators of points of service solutions have a solution where they can raise issues, and follow-up on the status of those tickets.
- Enterprise Knowledgebases & Document management solutions are important for the management and dissemination of policies, circulars, technical documentation, or public documentation whilst maintaining a complete set of version history for documents.

4.3 Evolving the Blueprint

Technology is an ever-evolving discipline, and the DHP should evolve as new technologies and integration techniques arise. The structure of the blueprint and its supporting documents (as described in section 2.3.1 on page 26) separates the concerns related to the blueprint into subordinate documents. This allows the documented function of the DHP components to evolve independently.

There will, however, be requirements for changing the enterprise architecture over time, and the blueprint proposes a mechanism to integrate and manage change (illustrated in Figure 26). This structure also applies to the development interoperability profiles and other assets. The proposed structure foresees three working groups aligned with the business domains in the blueprint:

- *Health Administration:* Concerned with those components in the Health Administration domain
- *IT Infrastructure, Privacy & Security:* Concerned with the components in the Shared Infrastructure and Privacy & Security domains of the blueprint
- *Health Delivery & Secondary Use:* Concerned with the components in the Health Delivery, Secondary Use and DHIW domains of the blueprint.

The blueprint also proposes three cross-cutting review committees to coordinate activities between these working groups:

- *E-Health Standards Review & Coordination Committee:* Comprised of Architecture Review Board (ArB), Privacy, Security & Ethics Review Board (PSErB), and the Health Systems Management Review Board (HSMrB). These groups provide review and input and guidance to the three working groups.
- *Implementable Technology Specification Group (ITSG):* Aligns the conceptual and logical views with the implementation technologies.
- *Certificate & Compliance Group (C&CG):* Concerned primarily with developing measures of compliance for implemented components (quality assurance).

The change management process begins with the submission of a change request from one of the working groups, or from an implementation partner, vendor, or institution.

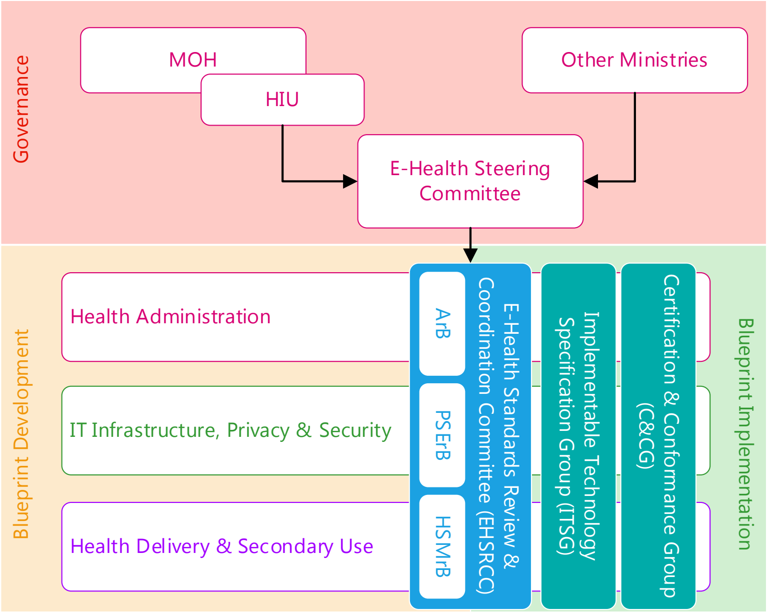

Governance
MOH
HIU
Other Ministries
E-Health Steering Committee
Blueprint Development
Health Administration
IT Infrastructure, Privacy & Security
Health Delivery & Secondary Use
ArB
PSErB
HSMrB
E-Health Standards Review & Coordination Committee (EHSRCC)
Implementable Technology Specification Group (ITSG)
Certification & Conformance Group (C&CG)
Blueprint Implementation

Figure 26 : *Blueprint Modification Structure*

The ArB should then review the change request during a regular meeting, and will identify the most responsible assignee for the implementation of the change. The scope of change is then classified:

- *Simplification:* A change to an existing component which is intended to clarify its meaning.
- *Incremental Change:* A new component or an addition an existing component or section which does not impact its role or functioning.
- *Re-Architecture Change:* The change represents a rewrite or change of an existing component which changes the way it or the blueprint operates.

If necessary, the responsible working group will consult relevant stakeholders (implementers, vendors, ministries, etc.) to validate the requirements of the change.

Once complete, a draft is reviewed by the ArB, PSErB, and HSMrB, followed by a final review by the EHSC/HIU. If no changes are required a new version of the blueprint document is published. If changes are identified, they are re-routed through the change management process. If no changes are required to the draft, then a new, amended version of the blueprint is published. An overview of this proposed process is shown in Figure 27.

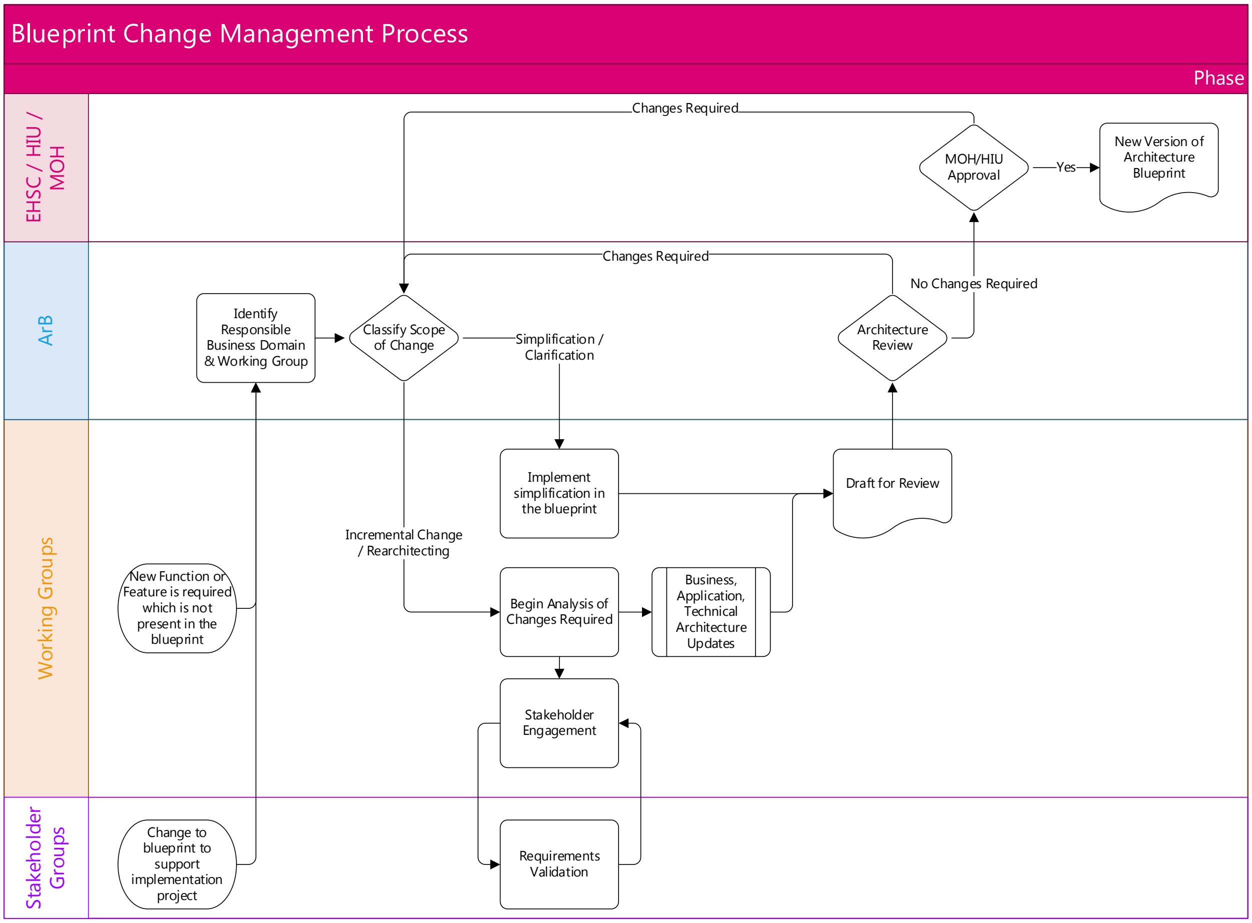

Blueprint Change Management Process
Phase
EHSC / HIU / MOH
ArB
Working Groups
Stakeholder Groups
Changes Required
MOH/HIU Approval
Yes
New Version of Architecture Blueprint
Changes Required
No Changes Required
Identify Responsible Business Domain & Working Group
Classify Scope of Change
Simplification / Clarification
Architecture Review
Implement simplification in the blueprint
Draft for Review
Incremental Change / Rearchitecting
New Function or Feature is required which is not present in the blueprint
Begin Analysis of Changes Required
Business, Application, Technical Architecture Updates
Stakeholder Engagement
Change to blueprint to support implementation project
Requirements Validation

Figure 27 : *Blueprint Change Process*

Implementation of new components will follow a realization plan (in the same pattern as the initial implementation of blueprint components). Changes or modifications to existing parts of the blueprint will manifest as new versions running alongside the existing components until the previous version may be retired (i.e. all services have been updated). This keeps with the principle of Evolutionary Development.

5. Information Architecture

5.1 Current State

The current state information architecture was adapted from the Digital Health Enterprise Architecture Plan [1] and summarised in this document for completeness (Figure 28). It provides a high-level overview of the structural design of shared health information in Sri Lanka. The primary information convergence points are the Ministry of Health and non-MOH Ministries for scoping data and depicts both electronic and paper-based information systems.

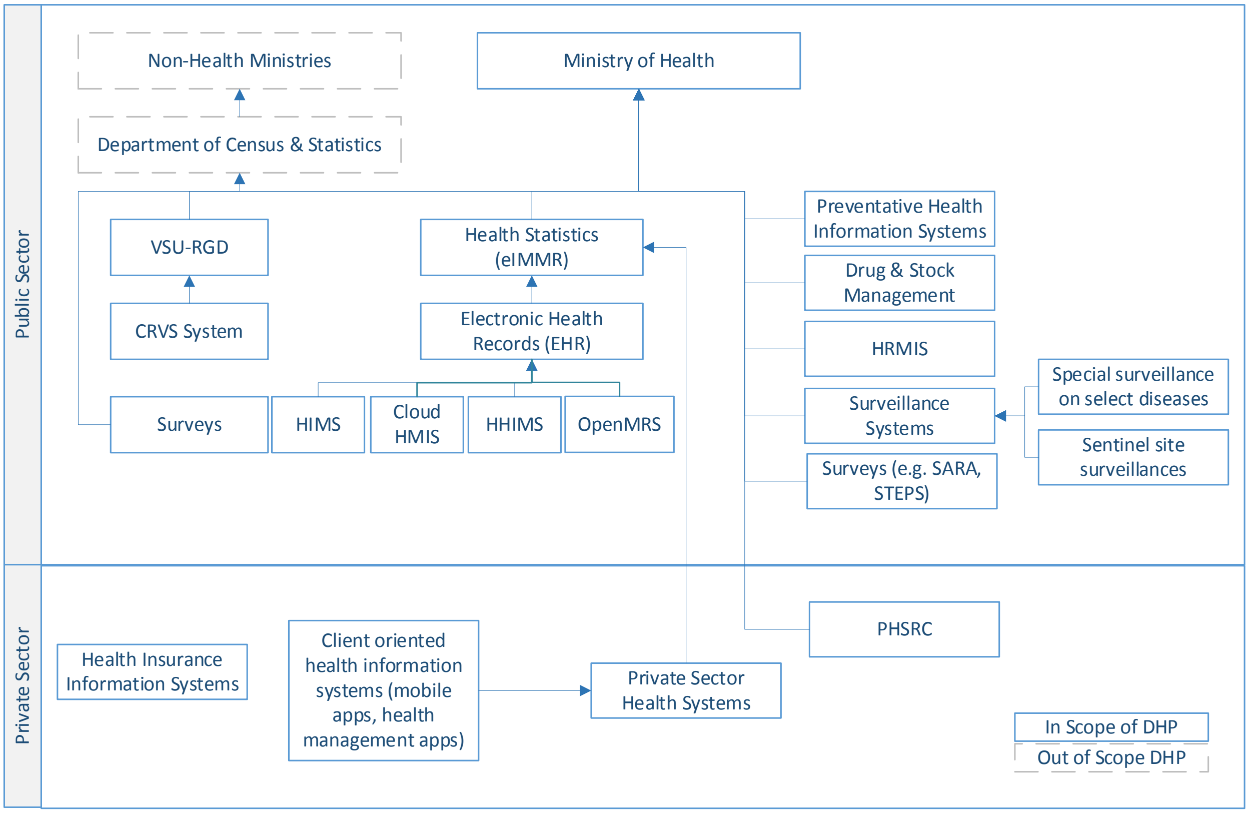

Public Sector
Private Sector
Non-Health Ministries
Ministry of Health
Department of Census & Statistics
VSU-RGD
Health Statistics (eIMMR)
CRVS System
Electronic Health Records (EHR)
Surveys
HIMS
Cloud HMIS
HHIMS
OpenMRS
Preventative Health Information Systems
Drug & Stock Management
HRMIS
Surveillance Systems
Surveys (e.g. SARA, STEPS)
Special surveillance on select diseases
Sentinel site surveillances
PHSRC
Health Insurance Information Systems
Client oriented health information systems (mobile apps, health management apps)
Private Sector Health Systems
In Scope of DHP
Out of Scope DHP

Figure 28 : *Baseline Information Architecture*

The public sector's preventative service information streams have matured for over a decade, and the information channels can be logically grouped into programmatic and surveillance information. Programmatic information follows program-specific monitoring activities such as Immunisation, Nutrition, Mental Health, Cancer, and others. Disease surveillance includes active and passive surveillance for communicable diseases, vaccine preventable disease, and other vector borne diseases.

Surveys are conducted by Ministry of Health including the Service Availability and Readiness Assessments (SARA), the STEPS non-communicable disease risk factor survey, and facility surveys. Additionally, surveys are conducted by other ministries such as the Demographic Health Survey (by Department of Census and Statistics).

The primary method of electronic data capture within Sri Lanka is the Health Information Management System (HIMS) SWASTHA and the Hospital Health Information Management System (HHIMS) which are responsible for gathering information within the public government curative settings. Summary records are generated from these and sent to the electronic Indoor Morbidity and Mortality Record (eIMMR) either in an automated or manual method of generation.

Other disease specific registries are maintained with various levels of organisation which were not evaluated within the current state analysis (such as stroke, vascular registry, CKD, and others).

Information flow of curative and preventative services is interspersed with information provided via supportive services. These include blood transfusion services, and other data streams such as laboratory information, drug &

stock management, administrative information, human resources, education and training, and financial information which is directly provided to MOH. These flows have a weak association with those in the curative and preventative health sectors.

5.1.1 Private Sector / Insurance

Private sector actors play an important role in the health information ecosystem of Sri Lanka. Private sector solutions provide mortality and morbidity data to the eIMMR system and are linked with various client-oriented health information systems deployed within private health institutions. It is important to identify private health insurance industry currently contains a rich source of verified health data which flows between providers and policy holders. These flows are not linked to the ministry of health or any government bodies.

5.2 Proposed Future State

The solution proposed by this document in section 3.3, organises areas of concern within a series of business domains. These business domains provide an overall grouping of logically related functionality for a future state digital health platform.

5.2.1 Enterprise Entities & Relationships

The enterprise blueprint provides an enterprise view of logical information entities and their relation to one another. Figure 29 provides an illustration of the high-level enterprise entities considered for management within the DHP and logical relationships to one another.

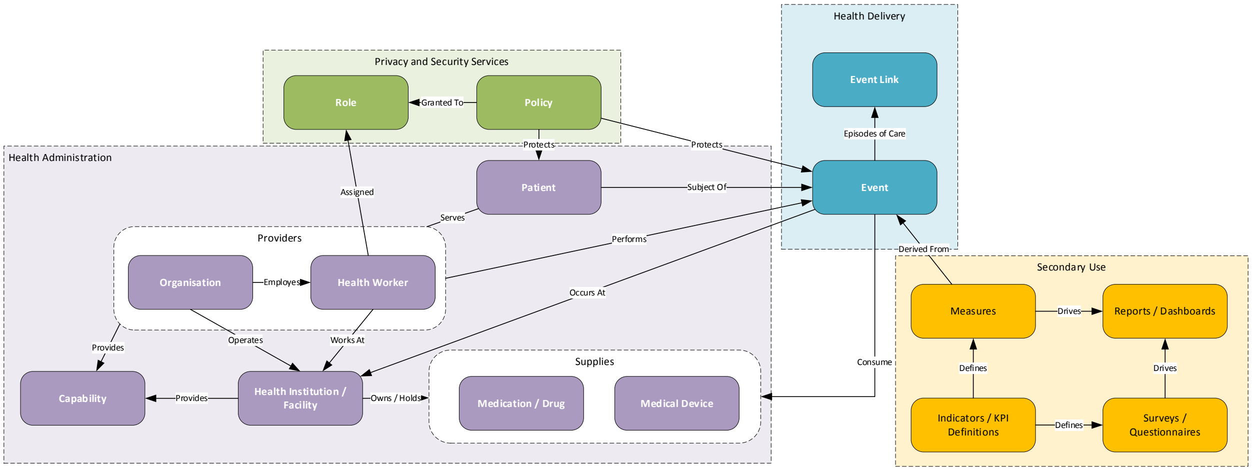


Figure 29 : *Enterprise Data Entities and Relationships*

Government insurance programs like the National Insurance Trust Fund (NITF) have more loose information flows to/from public and private healthcare institutions, and these are linked by the Ministry of Finance. The Private Health Sector Regulatory Commission (PHSRC) supports the linkage of information statistics from private institutions to the Ministry of Health.

The responsibility for managing the components of the logical data model lay with the business services defined in the DHP.

Entity	cription	ice(s)	DHGS Ref [2]
Role	Governed roles which a user, or health worker plays within the enterprise (i.e., General Staff, Patient Administration, HIV Specialist, etc.)	Identity Provider	
Policy	A defined access or action policy which are granted to roles and assigned to sensitive patient data within the DHP (examples: General Information, Taboo Information, No Secondary Use, VIP Data, etc.)	Identity Provider, Consent Management Service	
Patient	The recipients or clients of care.	Master Patient Index	7.2
Providers	A logical grouping of organisations and people from whom care is received by a patient.	Provider Registry	7.4
Health Worker	Physicians, Nurses, Medical Officers, Community Health Workers, Specialists, or other medical (and non-medical) people who provide health services.	Provider Registry	7.4
Organization	NGOs, Private Medical Corporations, and units of the MOH (DDG Dental, DDG MSI, DDG PHSI, etc) which provide health services to patients. This may also include organizations that provide healthcare supporting services such as facility and equipment maintenance services, transportation services for patients and supplies, dietary services, etc.	Provider Registry	
Health Institution / Facility	Healthcare institutions such as hospitals, clinics, private imaging clinics, dental clinics, or other locations where services are delivered to patients.	Facility Registry	7.3
Capability	A standardised description of a service, certification, speciality, device/modality, surgery theatre, or other capacities that a provider or facility must deliver to a patient (used primarily in service discovery)	Provider Registry, Facility Registry	
Supplies	Materials which can be ordered, dispensed, installed, or used for the delivery of care (used for consistent inventory tracking, ordering, etc.)	Medication / Drug Registry, Medical Supply Registry	
Medical Device	A medical device which is installed or used to care for a patient such as prosthetics, insulin pumps, pacemakers, stomas, and other such devices.	Medical Supply / Device Registry	

Entity	cription	ice(s)	DHGS Ref [2]
Medication / Drug	A substance which can be prescribed, administered, or dispensed to a patient.	Medication / Drug Registry, Inventory and Logistics Data	
Event	A Health Care Event ("Event") is a healthcare act of service or clinical interaction that is worth noting. An event normally represents the performance of some health service activity, possibly in accordance with a request or service definition. An Event can be an isolated interaction or a part of a multi-step workflow, process or clinical guideline. An Event can be in the past, present or future. The DHP is used to track Events which should, will, did or did not occur to the patient and which are clinically relevant for sharing between care settings and providers, or relevant for reporting purposes. These can be requests (orders), best practices (CDSS), scheduled events (intend to occur), occurred events, goals, or documents/summarisations which describe such events.	NEHR Repository, Medical Imaging Repositories, Disease / Domain Repositories, Document Repositories	7.7
Event Link	Links which occur between Event occurrences. These are used to track clinical order management (from request, to promise to fulfilment), stock flows (order, despatch, and receipt), links between visits (for chronic care, or disease care), as well as hospitalisation (admission to discharge)		
Measures	Values which are aggregated from care delivery events or captured discretely via surveys and questionnaires upon which management decisions are made.	DHIW	
Surveys / Questionnaires	Defined facility, organisation, or provider questionnaires for secondary use (example: number of operational fridges, planned outreach sessions, etc.) which must be gathered manually.	DHIW	
Indicators / KPI	The definition of measures which are to be observed from the health system. These can be computed indicators/KPI, or indicators which are collected manually from health institutions via surveys.	KPI Repository	

5.2.2 General Pattern of Information Flows in the DHP

The pattern of exchange between systems within the DHP will vary depending on the profiled standards used. However, regardless of the business trigger, and/or standard used, there is a general pattern of information flows for transactions between applications within the DHP. This pattern of information flow within the DHP is illustrated in Figure 30. Information flows where client and server TLS authentication (node authentication) are required are illustrated in purple.

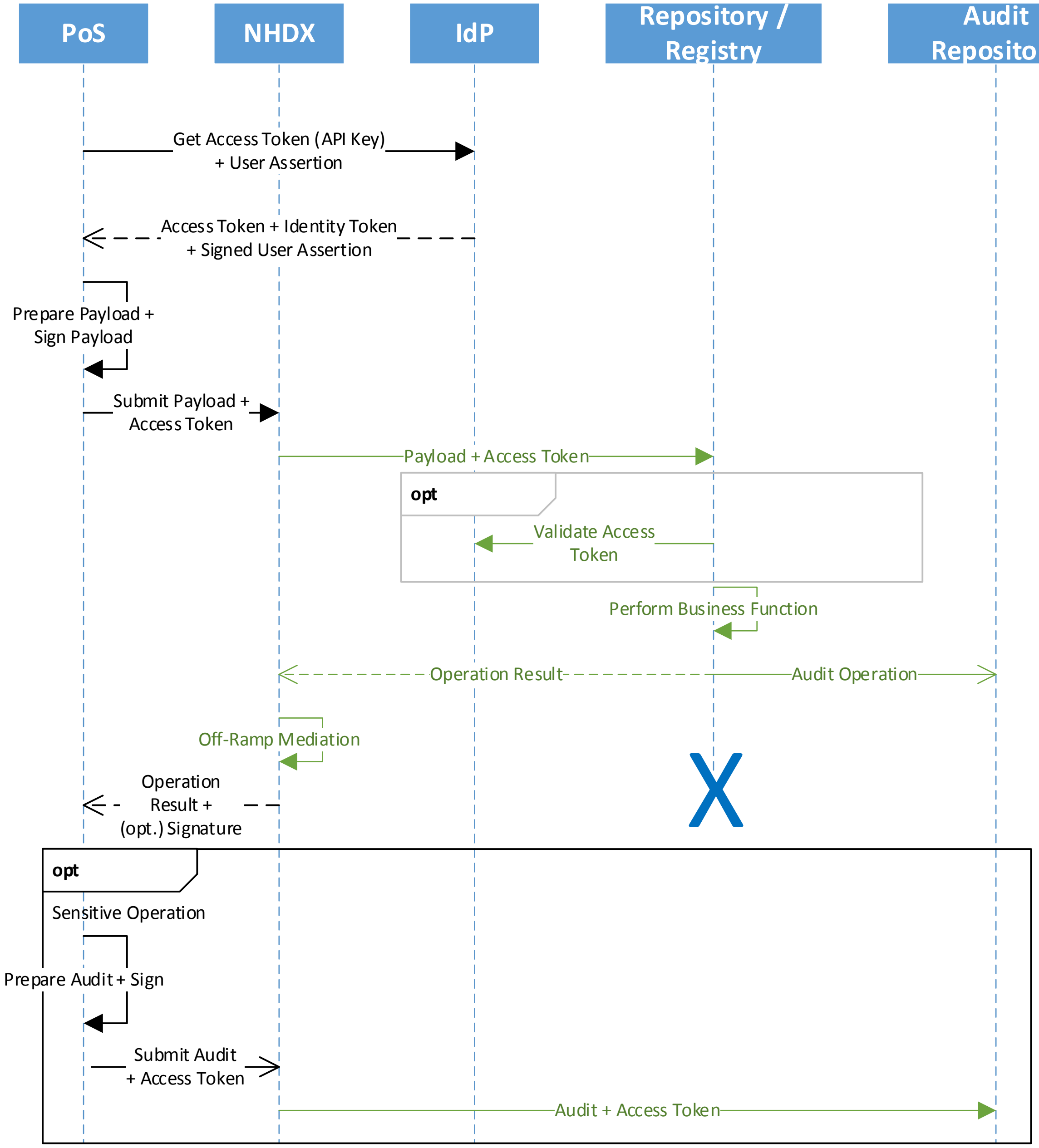

PoS
NHDX
IdP
Repository / Registry
Audit Repository
Get Access Token (API Key) + User Assertion
Access Token + Identity Token + Signed User Assertion
Prepare Payload + Sign Payload
Submit Payload + Access Token
Payload + Access Token
opt
Validate Access Token
Perform Business Function
Operation Result
Audit Operation
Off-Ramp Mediation
X
Operation Result + (opt.) Signature
opt
Sensitive Operation
Prepare Audit + Sign
Submit Audit + Access Token
Audit + Access Token

Figure 30 : *General Information Flow of Data Through the DHP*

The overall process flow is:

1. Obtain an authentication token from the central identity provider with appropriate scope (for the application, or user depending on the authentication context)[108]
2. Generate the payload to be sent to the server and digitally sign the payload using the device (and optionally the user's) signing credentials.
3. Call the NHDX service endpoint with:
    a. The device's issued client certificate (client TLS),
    b. The identity token obtained from the identity provider,
    c. The message header information if appropriate (trigger event id, message id, purpose, etc.),
    d. The signed data payload.
4. The NHDX will perform necessary on-ramping / receive mediation such as:
    a. Validating the message structure
    b. Validating the API access for the requesting system
    c. Logging the message receipt and identification
    d. Notifying subscribers of the message receipt
    e. Adding internal tracking or correlation data
5. The NHDX will route the message to one or more appropriate repository or registry services keeping the original authentication context (bearer token) intact.
6. The registry or repository service will perform whatever business tasks is needed to execute the instructions in the payload.
7. After completing the operation, the registry or repository will audit that it has completed requested task and will return the appropriate response to the NHDX
8. The NHDX will perform any off-ramp mediation which includes:
    a. Logging the response / result,
    b. Validating the message response,
    c. Masking or removing internal tracking / correlation data.
9. The NHDX will return the result of the operation (the acknowledgement) to the original point of service application which will then perform whatever business function it desires.
10. If indicated in the interoperability profile, the Point of Service audits the operation on the NHDX.

5.2.3 Health Events

The NDHGS [2] document defines the minimum dataset for the NEHR. The minimum dataset for the NEHR is primarily focused on the following key transactions:

- Healthcare Encounter (Admission, Visit)
- Laboratory Test Results
- Imaging Examination Results
- Medication Administrations
- Medication Dispensing
- Procedures
- Discharge Summary
- Death Declaration

The blueprint considers these transactions and their component data elements, as the basis for further extension to an enterprise information model for health event entities in the blueprint shown in Figure 31.

[108] IUA (ihe.net)

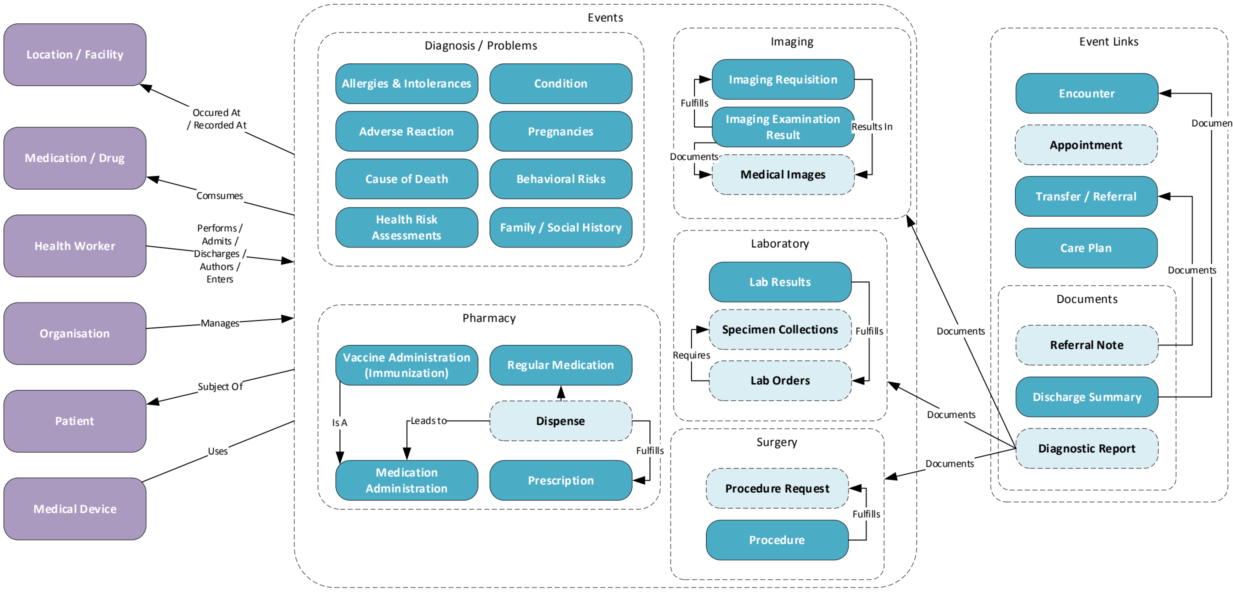


Figure 31 : *Event Information Model*

The concepts which are extensions of the NEHR model are illustrated in lighter colours, and high-level relationships are shown between relevant entities.

5.2.4 Security Audits

The information model for security is illustrated in Figure 32, and based on several sources include IETF RFC-3881[109], NEMA DICOM Section A.5[110], and HL7 FHIR[111].

The focal entity for the audit event is a description of the event that occurred. This includes the exact timestamp that the event was detected, the transaction that was performed, the classification of the event operation (create, read, update, delete, or execute), the classification of the event (query, run job, import, export, etc.).

The audit events are linked to the security identities which were involved in the performing of the event. These are important for identifying "who" was involved in the event and the nature of the role in the event. Audits will typically have the following actors specified:

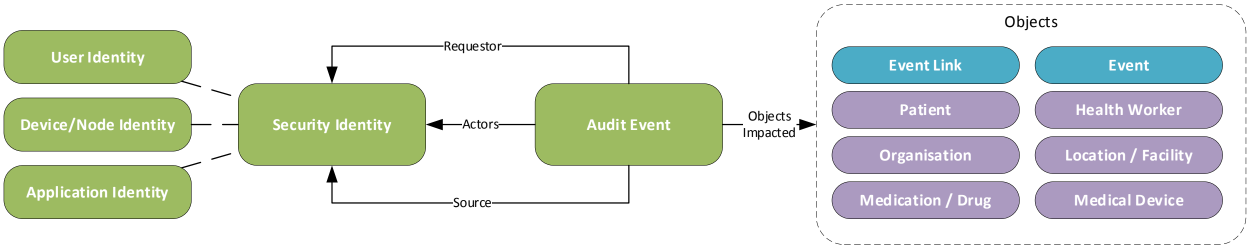


Figure 32 : *Logical Information Model for Audits*

[109] RFC 3881 - Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications (ietf.org)
[110] A.5 Audit Trail Message Format Profile (nema.org)
[111] AuditEvent - FHIR v4.3.0 (hl7.org)

- The source of the transaction (the sending system's IP address, and security identifier).
- The destination of the transaction (the recipient system's IP address, and security identifier).
- The user who made or initiated the event.
- Any proxy or routing information (the contents of any forwarding information) as it allows for tracing back to the original source of the request.

Additionally, an audit must identify an audit source, which describes the system which detected the event (the registry, the NHDX, the repository, etc.) which provides context as to the origin of the audit.

Finally, audit events should include the list of system objects or resources which were impacted in the event. The object impacted relationship should contain the identification of the object which was impacted (its resource id), the nature of the change (see 5.2.6.3 on page 114), and any other classification data which helps identify the object.

The list of events which trigger audits should be specified in the solution views for each transaction with the DHP infrastructure, as well a common system event such as:

- The service or software has been started or stopped.
- The service or software has begun or stopped recording audits.
- A user has authenticated themselves or logged off.
- Attempts to perform invalid executions are performed.
- The service or software configuration has been changed or modified.

5.2.5 Secondary Use

As described in section 4.2.6 on page 90, there are a variety of methods in which information may flow from primary points of service applications to the digital health information warehouse for subsequent use in a variety of secondary use cases. These information flows mimic current information flows between disease specific programmes, and the Hospital Information Management System (HIMS) SWASTHA, Hospital Health Information Management System (HHIMS) and Cloud Hospital Information Management System (cHIMS) to the electronic Indoor Morbidity and Mortality Register (eIMMR).

5.2.5.1 Secondary Use Information Flows

5.2.5.1.1 Submission of Aggregate Data

In this pattern, an information source (such as HHIMS or the NEHR Record Repository) downloads or otherwise obtains (and is configured) with one or more KPI definitions from the KPI definition registry and sends appropriate data to the DHIW (in FHIR parlance this is a Measure[112] definition).

This pattern of data flow matches the current flows from HHIMS, HIMS and CloudHMIS to the eIMMR with the exception that the target is a general purpose DHIW solution (i.e., all aggregate indicator reports are sent to one DHIW rather than multiple aggregate reporting systems), and that indicators are sent via the NHDX. Additionally, the use of digital signatures should be used to indicate that values submitted have been reviewed and "signed" as accurate.

On a regular basis, source system will use this definition to compute or calculate the output values based on information which is stored within its own data store. The results of this calculation are then sent as aggregates to the DHIW.

[112] Measure - FHIR v4.3.0 (hl7.org)

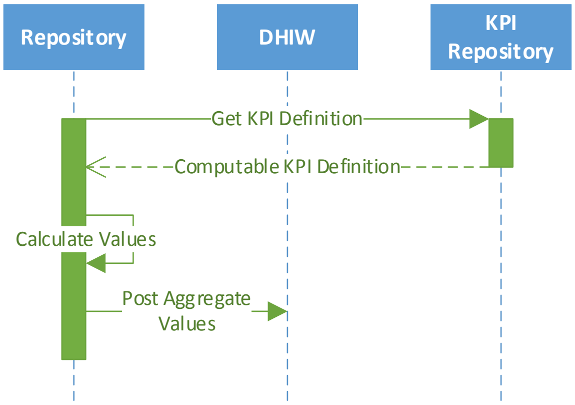


Figure 33 : *Automated Aggregate Data Exchange Pattern*

This information flow should use ADX[113] , HL7 FHIR MeasureReport[114] resources. There

5.2.5.1.2 Submission of Questionnaires / Surveys

This pattern aligns with manual data capture of indicators within for programmatic and surveillance tracking. In this pattern, a central repository of surveys (in FHIR parlance Questionnaires[115]) is obtained by a compatible digital health solution.

A user then completes the survey for the reporting period and submits the completed survey (QuestionnaireResponse[116]) to the NHDX for population of data within the DHIW.

5.2.5.1.3 Extraction, Transform, Load (ETL)

Another information flow from a source repository within the DHP to the DHIW is the use of traditional ETL patterns.

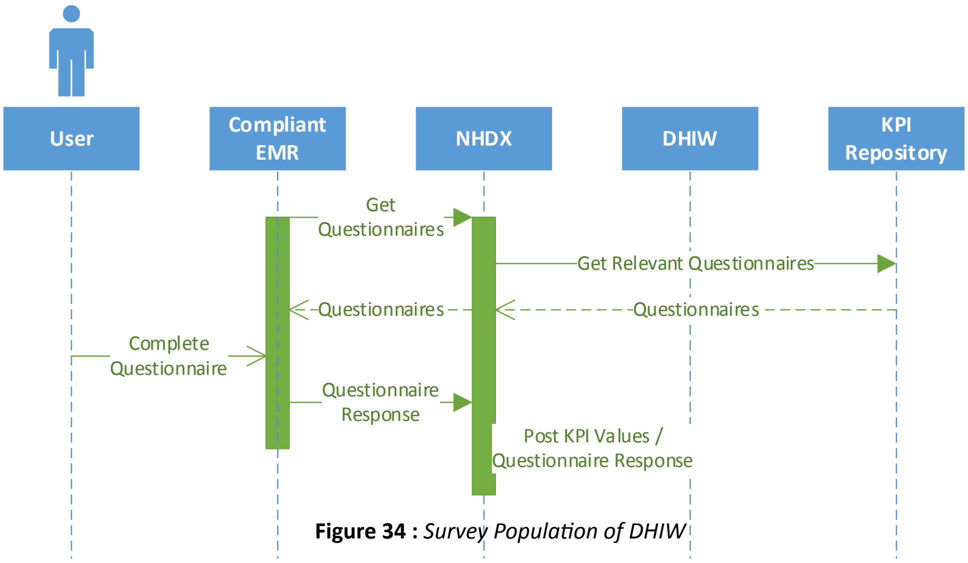


Figure 34 : *Survey Population of DHIW*

[113] Aggregate Data Exchange - IHE Wiki
[114] MeasureReport - FHIR v4.3.0 (hl7.org)
[115] Questionnaire - FHIR v4.3.0 (hl7.org)
[116] QuestionnaireResponse - FHIR v4.3.0 (hl7.org)

In this pattern, a dedicated ETL provider service will query data from one or more repositories within the DHP on a regular cadence and will perform aggregations, de-identification, pseudonymisation or other processes before pushing data to the DHIW.

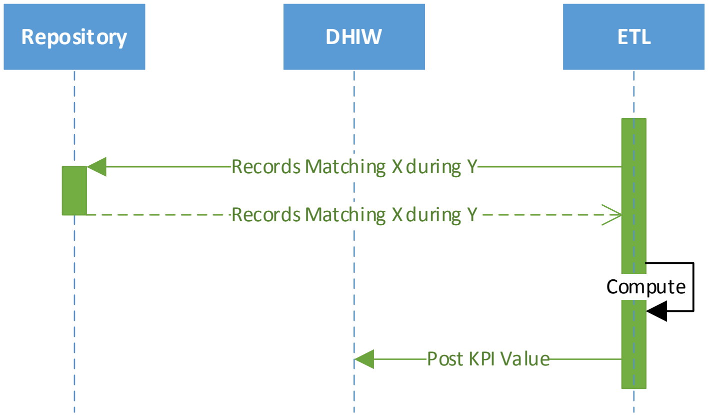


Figure 35 : *Using ETL to Populate DHIW*

5.2.5.1 *Near-Real-Time Reporting*

Another pattern of populating secondary use data Near-real-time calculation of KPI values directly from events which occur through the NHDX or service bus using subscriptions on the service bus (example: whenever a positive diagnosis of Dengue is suspected, the public health department is notified).

The blueprint proposes using FHIR Subscriptions[117] for management of subscriptions. The notification of the backing system (in this case the DHW) is a rest hook or push notification target.

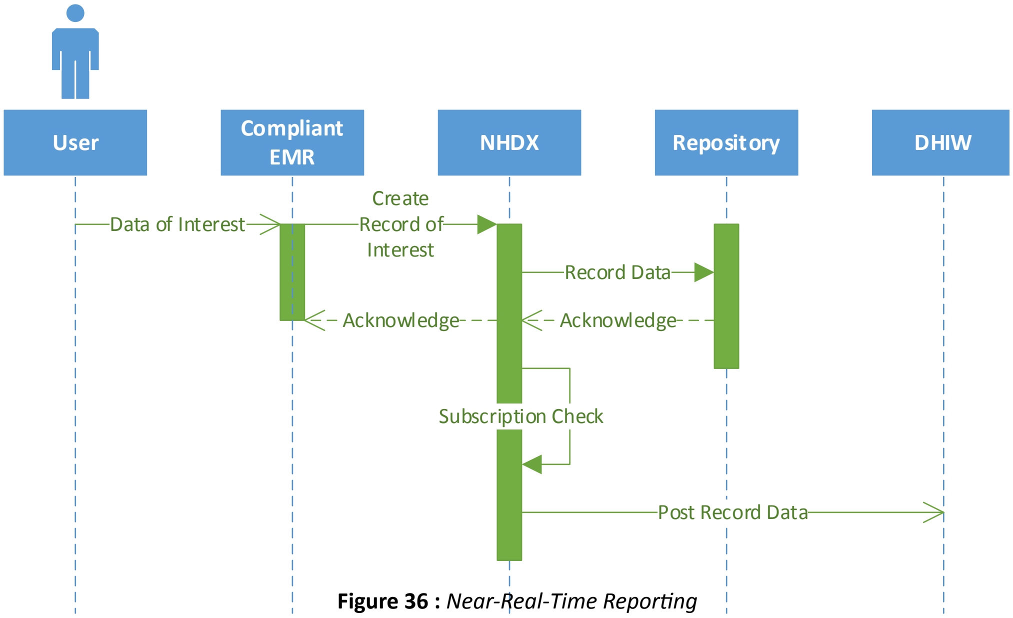


Figure 36 : *Near-Real-Time Reporting*

[117] Subscription - FHIR v4.3.0 (hl7.org)

5.2.6 Information Management Principles

5.2.6.1 Data and Information Policies

The information which is created, amended, and disclosed does not exist in a policy vacuum, and the creation and use of sensitive information should be considered whenever data is exchanged between organisational boundaries. All participants within the DHP should define and share information policies related (but not limited) to:

- *Data Sharing Policy:* Documentation related to the intended use of information stored within the DHP, and the expectations of quality. Additionally, data sharing policies should set forth constraints or grants on disclosure, delegation of responsibility, and requirements for auditing and accessibility.
- *Data Retention Policy:* Documentation and tagging related to the archival and disposal of data within the enterprise. This includes how long, for example, data is relevant to reside in the patient's record, as well as the expectations of retention within points of service. Policy should also set forth appropriate methods for archival, retrieval, and destruction of data based on events (death, birth, etc.), time limits (delete within 5 days of download or transfer) or use limits (delete immediately after using).
- *Disclosure Labels and Policies:* Data stored within the DHP in the NEHR or other registries and repositories should have security and policy labels appended directly to the information (as an example, FHIR defines security labels for data[118]). All participants on the DHP must adhere to these tagged disclosure policies and should take appropriate action (masking, redaction, removal, etc.) to appropriately enforce these policies. Disclosure and security labels MUST NOT be removed from information when downloaded locally within a point of service.

Further technical discussion about consent directives and disclosure/capture policies is contained in section 6.2.10 on page 128.

5.2.6.2 Maintenance of Metadata

Metadata refers to information about a primary set of data which provides additional information on a resource such as:

- What is the version of the resource which has been accessed?
- What was the last time the resource was modified?
- What is the status of a business workflow being actioned on this piece of information? (Is it approved, preliminary, etc.)
- Where did the object originate from? (it's provenance)
- What was the intended purpose of the data?

The format and structure of this metadata will depend on the originating structure, for example HL7 FHIR resources use the Meta property[119] on a resource, whereas DICOM objects use metadata elements[120]. Regardless of the originating format and structure, metadata which is received, generated, and disclosed to points of service should be stored and associated with the original data to which it was attached whenever it is transferred.

5.2.6.3 Information Lifecycle Management

Information, which is provided to the DHP, whether in the NEHR or other repositories and registries, follow a common lifecycle. Whenever auditing access, disclosure, or updates to clinical information within the DHP, it is important that audits, processes, and logs understand the lifecycle event which occurred.

[118] Valueset-security-labels - FHIR v4.3.0 (hl7.org)
[119] http://hl7.org/fhir/resource.html#Meta
[120] 7 Registry of DICOM File Meta Elements (nema.org)

IETF RFC3881[121] provides a complete series of states for the lifecycle of health information, and a useful subset is summarised in Table 2.

Table 2 - Information Lifecycles

Lifecycle Stage	Description	Examples
Creation / Origination	The clinical information was created based on a real-world event or observation.	Recording Weight of Patient
Import / Copy of Original	The clinical information was created as a copy of another record.	NHDX receiving information from an EMR
Amendment	The clinical information was amended with updated values. Whether the original copy exists will depend on the capability of the repository storing the data. Since triggers and third-party systems should have been notified of the original and already taken actions on it, it is important to understand the amendment or change of data over time.	User corrects a lot number of a vaccination event.
Verification	The clinical information was verified by a third-party system, or solution.	A physician has reviewed the data and has certified it to be true.
Translation	The clinical information is not as represented in its original form, however, is a translation of the information format. This is useful from a medical/ legal perspective since it indicates that a computer process (or third party) has changed the structure of the data from original.	The NHDX upgrades a message from FHIR R4 to FHIR R5
Access	The clinical information is being accessed by a system process, job, ETL, for internal processing.	A matching process in the MPI reads a clinical record for its de-duplication logic.
De-Identification	The clinical information represents a copy of an original where identifying information was removed, pseudonymised, or fuzzed to protect the identity of the subject of care.	An extract of sample data for a research study.
Aggregation or Derivation	The clinical information was aggregated into a derived form (if referencing the derived data, the information was derived from a source)	Generating an indicator measure from a KPI definition.
Export / Copy to Target	The clinical information is being exported and sent to another system (in original form)	A PACS sending an image to another point of service.

[121] RFC 3881 - Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications (ietf.org)

Disclosure	The clinical information was being disclosed to an outside system, user, organisation, etc.	A patient record which appears in a demographics query initiated by a physician.
Archiving	The clinical information has been archived as part of a data retention or backup procedure.	Data through a retention service has been removed from primary storage to an offline, long-term backup archive.
Logical Deletion	The clinical information has been flagged as "deleted" and does not appear in live search results and is not available for discovery by users or services. The information still exists in the physical data storage technology.	An observation entered in error is withdrawn.
Permanently Erased	The clinical information has been purged from the physical data storage. It is no longer available.	Data about a patient is purged.

5.2.6.3.1 De-Identification

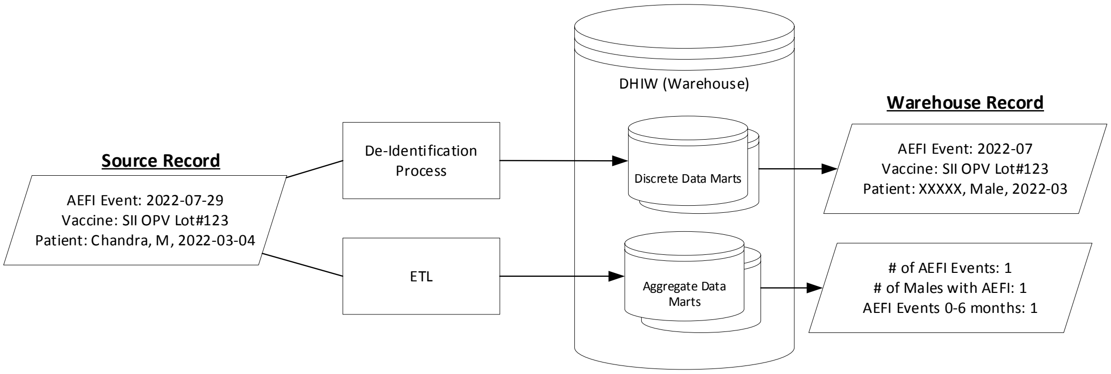


Figure 37 : *Data Flow for De-Identification*

Whichever techniques are employed however, de-identified data can still be full of identifying information and will still need extensive privacy protections. The design and operation of any de-identification profile or system must be validated and monitored.

The NDGS identifies the need for de-identification procedures in 6.2.2 however does not specify the methods of this de-identification due to the varied secondary uses of data. A comprehensive practical approach to the de-identification of data is provided in the IHE De-identification Handbook[122].

5.2.6.4 Referential Integrity Between Services

In an enterprise environment where information is exchanged between organisations and systems, referential integrity of data becomes increasingly difficult. Links contained in events which point to different repositories, registries and points of service will degrade over time unless care is taken to prevent this.

For example, one can imagine a scenario for a pancreatic cancer diagnosis. In the NEHR, such a diagnosis would contain:

[122] https://wiki.ihe.net/index.php/Healthcare_De-Identification_Handbook

- Codes which indicate the diagnosis, finding site, prognosis, etc. (ICPC, ICD, etc.)
- A link to the patient identity (in the Master Patient Index)
- A link to the organisation which authored the diagnosis (in the Provider Registry)
- A link to the facility/location where the diagnosis was made (in the Facility Registry)
- A link to a treatment/care plan
- A link to the person who entered the data, performed the test, authored the result report
- A link to the diagnostic image order, result, reports which was used to form the diagnosis (in the source RIS/PACS)

If these links are stored on different solutions, they may become unavailable over time due to a variety of reasons:

- The software solution may be temporarily unavailable (due to maintenance, configuration change, etc.)
- The data may have been archived and/or purged for retained information, or may have been logically deleted and is no longer available[123]
- The data may have been moved or its security tags/policies changed since the original reference to the remote server was made and the reader system may not have access to the updated resource (under the new security policies)

A consumer of this information would have only a partial picture of the health event. This problem is especially difficult to maintain if using HL7 FHIR outside of SOA patterns[124].

To mitigate this type of condition, the blueprint proposes that all exchanges of information and all data storage within the DHP services will:

- Encapsulate all the data submitted to the DHP in a single transaction bundle (see section 6.2.5 on page 123)
- Avoid using permanent erasure of data, and provide logical deletion of data (i.e., prevent discovery of old data, however, allow direct retrieval, where possible)
- Store summary or snapshot data of the referenced data and provide narrative description information for the reference[125]
- Store and reproduce the entirety of the resource/record text (i.e., structural data will be unavailable, but in-context narrative is available)[126] when queried, so that a human reading the information can be provided a complete context of the event which occurred.

[123] Http - FHIR v4.3.0 (hl7.org)

[124] Services - FHIR v4.3.0 (hl7.org)

[125] References-definitions - FHIR v4.3.0 (hl7.org)

[126] Domain Resource - FHIR v4.3.0 (hl7.org)

6. Technology Architecture

This section describes the technical and functional principals for components within the blueprint.

6.1 Technical Principles

This section describes the technically oriented architectural principles that are to be used when designing solutions based on the Blueprint. Solutions that align to these principles offer a fundamental level of compliance to the Blueprint architecture. Components, services, or applications that are not in alignment with these principles will considered be non-conformant to the Enterprise Architecture Blueprint.

6.1.1 Privacy and Security Control by Design

A Citizen should have full awareness and be in control of the collection, processing and use of health data related to them. Where possible data should be shared through links that refer to the original source of the data, or APIs that can provide near real-time access, rather than the use of data replication techniques to reduce duplication and storage of copies of data in multiple locations. Avoiding storage of unnecessary copies of data assists in data governance by providing a "single source of truth" and helps to protect privacy by limiting data proliferation and unnecessary exposure.

Specifications for data and information exchanges must clearly identify the privacy and security considerations of the data exchange, and should include mitigations (auditing, access control, policies, etc.) to guide implementation. All technology solutions should utilise AAA security - Authentication, Authorization, and Accounting as a security framework that controls access to computer resources, enforces policies, and audits usage. Systems should keep a detailed audit log of access, and disclosure to/from the enterprise infrastructure. Role-based user security controls and the ability to convey the identity of the end user performing an action should be integrated into all digital health solutions to ensure privacy, confidentiality, and ethical use of the digital health platform.

Health information should only be used with applicable permissions and consent, and systems should use a common (centralized) authentication architecture where possible, as opposed to a local authentication scheme. Regional or domain specific data hubs can be established to service groups of smaller facilities with limited infrastructure. Institutions that store information on behalf of another legal entity should enter into a data sharing agreement to establish terms and use of that information.

All technology solutions should be encrypted at rest and in transit. This is especially important where network traffic crosses organizational or jurisdictional boundaries. Exceptions to encryption can be made on a case-by-case basis if required, for example servers communicating on a private local network in a protected data centre. To protect the integrity of the healthcare system, systems must employ safeguards to defend against the broadest possible range of vulnerabilities.

The minimal amount of information should be collected to achieve the immediate clinical or business outcome – unnecessary or unused information should never be collected or stored.

6.1.2 Use of Open Standards and Open-Source Software

Services and information exchanges within the enterprise should be based on Open Standards[127] wherever possible. Implementations shall make use of Free/Libre and Open- Source Software (FLOSS) where available[128]. Open Data for research and quality improvement to authorized parties where suitable should be shared. Applications will provide Open APIs to authorized parties where suitable.

Solutions must support open standards and platform independent protocols to provide long term stability and interoperability whenever possible. Designs should prioritize the creation of interoperable vendor-neutral solutions. All components of the Blueprint should leverage well documented, non-proprietary, and Open Standards using platform independent protocols (such as HTTP, XML, JSON, etc.)

Wherever possible, openly available data and integration standards and technologies should be used as specified without customization. If this is not possible, adaptation of the standard (using profiling or extension) can be done. Custom, ad hoc, or single-purpose data integration interfaces should be discouraged. Reuse and improvement of existing assets (specifications, designs, software source code, components, etc.) is encouraged for maximum utilization of available resources. Leveraging expertise and building from successes, documenting, sharing, and making use of best practices and reusable artifacts, components, services, and processes across the entire ecosystem is highly encouraged.

[127] Definition of "Open Standards" (itu.int)

[128] National Digital Health Guidelines and Standards [2] Section 3.1.3

6.1.3 Interoperability Focus

The Blueprint promotes the adoption and use of appropriate interoperability standards (both technical and business) to enable quality, consistent data across the enterprise and with outside trading partners. This necessitates that all digital health components and solutions focus on interoperability as a key consideration of their design.

Interoperability standards will be defined for the correct use case, context, or workflow and will include structured data and terminology. Ensuring consistent business processes and data between organisational units ensures that information is captured/validated in a common way.

6.1.4 Re-Use Shared Business Services

Stakeholders will collaborate to select and define, where possible, reusable, and sharable common services to support functionality across the enterprise and across health domains to help the citizens of Sri Lanka.

Whenever possible, components and solutions within the digital health ecosystem will utilize existing service components rather than re-implementing custom services to achieve the same business objectives. Digital health solutions should also seek to expose and share their data with the DHP infrastructure.

6.1.5 Leverage Virtualized and Cloud Design Patterns

All technologies within the digital health enterprise should seek, whenever possible, to virtualize all implementations using appropriate shared infrastructure and/or cloud-based technologies. Use of cloud-based technologies whenever possible should promote the accessibility, scalability, cost efficiency and monitoring of resource use.

Shared infrastructure reduces costs of migration, improves security through centralized control, and improves scalability through the ability to dynamically assign resources as needed. Data sharing agreements should be developed with any third party managed service that houses health information, and the physical location and subsequent legal jurisdiction(s) of the data storage should be clearly articulated. Designs must also consider resiliency in the case of network outage or loss of internet access and offer contingency plans for inevitable cloud outages.

6.1.6 Line of Business Systems are Expert Systems

When designing the enterprise architecture and domain specific applications, the line of business systems (e.g., Master Patient Index, Facility Registry, eIMS-SL, etc.) should be considered the authority in their domain, as they are assumed to be designed in consultation with the clinical and administrative experts within their domain. The role of the central infostructure is primarily to orchestrate, translate, reliably deliver, and govern exchange between these expert systems. Where possible, the infostructure should not attempt to re-create the business processes of a clinical or administrative domain. This separation of concerns greatly reduces complexity of the integration environment.

6.2 Functional Principles of Digital Health Solutions

This section introduces the minimum common functional principles of components operating within the infrastructure that is developed within the digital health solution.

6.2.1 Non- Repudiation of Information

A patient's national electronic health record (NEHR) represents a collection of discrete data events which are contributed to the digital health platform by a variety of providers and systems. This data is also used to drive health measurements and key performance indicators (KPIs), clinical decisions and other business functions upon which erroneous, false, or modified information may have an adverse impact.

The principles of non-repudiation of information, when used ensure:

I. Accurate and correct as reviewed by a medical professional prior to submission
II. Originates from a known, identified source and the data in the enterprise matches the data submitted from the source.

Has a known provenance/origin which identifies the context in which the data was created?

6.2.1.1 Non-Repudiation of Emission

It is therefore important that data submitted to the patient's NEHR is validated prior to submission and signed. This mechanism is known as non-repudiation of emission (NRE) and ensures the data has been verified and certified it to be true. The digital signature ensures that data is not altered after verification by the submitting provider.

6.2.1.2 Non-Repudiation of Origin

It is important to understand the origin of data after it is submitted to the enterprise. Understanding the provenance and of data (where it originated from, the reason why it originated, etc.) is paramount to validating information which may be incorrect and performing follow-up with the submitter.

It is also important that data submitted by the sender is known to be submitted by the origin and has not been altered since submission. This is known as non-repudiation of origin (NRO) and ensures that the data originated from a known source.

6.2.2 Portability for Digital Health Services

It is important, while designing any of the digital health services which comprise the digital health platform, that those systems are designed in a manner which prevents architecture assumptions or platform dependencies. For example, designing a solution to only work on Google Cloud by using GScripts or with proprietary Microsoft Azure APIs would represent a lock-in of that system to one environment which may or may not be under the control of the Ministry of Health of Sri Lanka.

When designing services or health solutions, care should be taken to ensure that:

- Proprietary operating environments and services are avoided, and generic alternates are considered (e.g., instead of using a proprietary solution such as Amazon S3 storage, use an open alternative such as WebDAV so the solution can be migrated if needed)
- At a design level, there should be no assumptions made based on the presence of another system or solution being available (e.g., the Provider Registry should attempt to avoid hard dependencies on the Client Registry – rather it should rely on the NHDX bus or message passing interface to facilitate connections such as this)

6.2.3 Identifier Management

The ability to resolve the identity of entities and events uniquely is a key challenge in achieving interoperability between multiple systems. Information systems that operate within the confines of a specific organisation can assign and manage identifiers within the scope of that organisation. However, once those systems start communicating and sharing information across those organisational boundaries to the broader enterprise, the possibility of information duplication and concerns about shared entities and events quickly becomes a problem.

This issue is especially acute in the health sector, where a history of compartmentalised (or siloed) systems, regional consolidation, and devolution of responsibility for service delivery, and the subsequent outcome of facility and information system rationalisation.

Use of enterprise identifiers for entities in the health infostructure is a foundational concept. The Patient UID, Institution UID, Medication UID, and Provider UIDs are managed by the Client Registry, Institution Registry, Medication & Device Registry and Provider Registry respectively. Enterprise identifiers should be meaningless but unique numbers (commonly referred to as MBUNs) never to be disclosed to users, rather used for internal linkages only.

Business Identifiers like National Identity Card (NIC), Sri Lanka Institution Number (SLIN), Personal Health Number (PHN) is issued and captured by other systems. These should be comprised of at least two parts when conveyed to the digital infrastructure – a system source identifier and an entity identifier.

All digital health services which are participants in the DHP should strive to use proper identifier management of providers, facilities, patients, organisations, materials, etc. Often, solutions will identify entities using an internal primary key and they will use this primary key for referencing data. Services within the DHS should use, where possible, business identifiers as the source of truth for identification of resources rather than local "primary keys" from source systems.

6.2.3.1 Enterprise Identifiers within the DHP

The digital health solution should strive to use common, internal enterprise identifiers which are used only within the DHP and linked to external identifiers using cross referencing functions of the Client, Provider, Facility, and other registries. The following guidelines should be used when designing enterprise identifiers:

- The generation of new enterprise identifiers must be handled only by the enterprise registry responsible for maintenance of the identifier (for example: enterprise client identifiers should only be generated by the enterprise client registry)
- The enterprise identifiers should be meaningless, unique identifiers (for example a UUID) which contain no personal identification information in the identifier.
- The enterprise identifiers should not be used external to the DHP or by systems not participating in the DHP. This means that the enterprise identifiers should not appear in user interfaces, point of service systems, etc.
- Enterprise identifiers are governed by the issuing system, only the system which has generated the enterprise identifier should be permitted to update primary or "golden" identities for the clients, providers, facilities, etc.
- New enterprise identifiers should only be generated for new clients/patients registered in the DHP, and should not be pre-generated, change or be retired unless by an internal MPI function of the client, provider, or facility registries after appropriate EMPI matching functions have been performed.
- One physical entity (a person, a facility, an organisation, a material, etc.) should have one and only one enterprise identifier. If a physical entity carries multiple identifiers (for example, multiple identifiers from licensing authorities) they will be linked to the one enterprise identifier for the object.

Specific details about the design and use of enterprise and business identifiers can be found in the Interoperability Plan.

6.2.4 Follow Standards and Interoperability Plan

Digital Health solutions should follow the Interoperability Plan for Sri Lankan digital health standards wherever possible[129].

[129] National Digital Health Guidelines and Standards [2] Section 3.1.2

Interoperability Profiles (see section 2.3.2 on page 27) will define:

- Trigger events which define when the point of service applications should contact the shared DHP infrastructure and for what purpose.
- Behaviours of the DHP services and the point of service applications consuming those services
- Expected auditing and security requirements (authorization and authentication) of the point of service and DHP service.
- Expected data elements for each trigger event and the associated minimum data set which accompanies the trigger event.
- Additionally, a Technical Guides (physical views) within the DHP blueprint will define:
- The concrete standards being used (example: FHIR JSON R4, DICOM, etc.)
- The concrete validation instructions expressed in the relevant standards selected (example: XSD, FHIR IG, etc.)
- Physical locations of services (examples: API endpoints, OAUTH scopes, etc.)
- Concrete security expectations (contents of audits, OAUTH patterns, auditing messages, etc.)

6.2.4.1 Normalisation of Data

There is a medical and legal liability introduced by systems which transform, translate, or modify clinical data submitted by point of service systems. It is important that what a clinician has signed as being true (see section 6.2.1) should not be modified. However, it is also important that this information be extractable and/or computable by any consumer of DHP data while maintaining the proper context.

It is therefore important that data in source systems be normalised according to the interoperability profiles prior to submission of this data to the DHP. This normalisation should ensure:

- Data submitted is unambiguous (see section 6.2.5), complete and in context as the source system (and submitting system understands it)
- All terminology used aligns to the correct terms specified in the interoperability plan (i.e., use of ICD10, SNOMED, LOINC, etc. as appropriate)
- All structures used conform to the minimum data sets specified in the trigger event definitions
- A human readable representation of data is submitted alongside the structured data (i.e., what the clinician sees is what is signed and submitted)

6.2.5 Encapsulation of Data Submitted

Whenever submitting data to an enterprise, the contents of the message may be transmitted, wrapped, queued and retried, etc. Because of this, with the exception of queries and reads, digital health services should refreain from using (RESTful) CRUD (Create, Read, Update, Delete) methodology when creating or amending data on the DHP.

APIs used in the DHP should ensure that they:

- Include message header information which identify the trigger event, the clinical rationale (if required), and a unique message identifier (to correlate responses, and retries).
- Include in the message human readable summaries of the data referenced in the clinical act including patient, provider, facility, medication, and terminology display names.
- Include contextual information as a snapshot of "current state of truth" at the time of the event. For example, if submitting discharge information from a hospital visit the submission should include the visit, summary observations, procedures, prescribed medications, etc. within the submitted bundle.
- Responses should include the request message identifier for which the response is acknowledging to allow enterprise

services to correlate requests and responses asynchronously.

An example of this pattern in HL7 FHIR is the Message exchange pattern[130].

6.2.6 Performance Targets

Performance targets in the future should cover both curative and preventive, including both public and private institutions. For example, there are more than 1,600 institutions in the state health sector alone in Sri Lanka which have the potential to use the DHP infrastructure to share vital clinical data between organisations. To be useful in a clinical environment the system must be available, reliable, and responsive, as well as aligned to clinical business processes.

6.2.6.1 Performance of DHP Services

DHP services will be composed and orchestrated in a variety of workflows within the DHP infrastructure. It is therefore vital that services operating within the DHP are available 24 hours per day, 7 days per week, with greater than 99.9% uptime and can respond to transactional queries (reads) within appropriate timeframes (typically less than 2 seconds is considered appropriate).

This general performance metric can only be reliably controlled within the DHP infrastructure itself. It is recommended that the following design techniques be explored and included in the design and deployment of DHP services:

- *Caching:* The DHP should use, where possible, short-term caches which can service reads without the need of orchestrating or contacting persistence layers. The most difficult part of caching is the expiration and eviction of objects which become "stale" from the cache, and this becomes much more difficult in a heterogenous environment. Cache durations should be configured based on the type of data and should (where possible) use appropriate versioning and/or tagging to allow for validation of a cache object prior to return.
- *Performance Clustering:* Where possible DHP services should be stateless, but where that is not possible services should also include methods of sharing states between nodes to allow for clustering of services. Strategies for clustering include round-robin or intelligent load balancing between application servers, and the use of synchronous replication of data tiers.
- *Failover Clustering:* All DHP services must be deployed in a manner which allows for failover clustering. Such clustering is required for maintenance of individual DHP services without introducing outages in the broader DHP infrastructure. Additionally, in the case of a single hardware or software failure, a backup node remains available for servicing requests.
- *SSL Termination:* HTTPS (HTTP over SSL) ensures that data is encrypted when it is transmitted between nodes. However, there are many instances within an enterprise architecture where the physical network is secured (via VPN, VLAN isolation, etc.) and where TLS adds additional burden to transactional processing between internal DHP services. SSL termination offloads encryption overhead and should when the DHP traffic transits a network that is physically secured, secured via lower layer network infrastructure (such as VPN or SSH tunnels), or transiting already encrypted channels (such as encrypted queues).

6.2.6.2 Performance between DHP and Points of Service

Performance targets are subject to a variety of factors including the size of the data payloads, the network bandwidth between the point of service applications and the DHP, and the load on the DHP infrastructure. To ensure timely access to national health record (NEHR) data from the DHP within

[130] Messaging - FHIR v4.3.0 (hl7.org)

points of service, the following strategies should be employed:

- *Pre-fetching of Data:* Many clinical events can be pre-fetched from the DHP using a variety of data sources including cohort/catchment attributes (i.e., patients in my village, patients assigned to me, etc.), intent or appointments (i.e., patients who are scheduled to present), or on trigger events (i.e., admission to hospital, etc.). Such pre-fetching should be implemented where clinically safe and should be audited and secured appropriately. Pre-fetching can be especially effective for large datasets such as medical imaging.

- *Compression of Data:* Whenever points of service request data from the DHP, they should (where supported) request that the DHP compress response payloads. While this introduces a slight computational overhead on the DHP and the PoS application, it significantly reduces network overhead when connection speeds are low.

- *Efficient Transfer of Large Objects:* The size of data payloads varies dramatically between clinical domains in healthcare. Special attention should be paid when developing solution guides and technical guides for various domains to take data sizes. For example, while patient demographic data is quite small (on the order of a few kilobytes), files for various modalities of diagnostic imaging files can range from a few megabytes to hundreds of megabytes or a few gigabytes per transmission, and images from high resolution digital pathology systems are often several gigabytes per file. When specifying the data transfer of large objects, profiles should use established methods of transferring large binary objects and refrain from transports requiring text encodings.

6.2.6.3 Support Agreements

All digital health solutions and points of service connected to the DHP, and services within the DHP, must have in place service level agreements (SLAs). Such agreements should establish:

- Appropriate performance measures including response time requirements to users to/from the DHP and internal services
- Availability requirements including downtime impacts and mitigations
- Maintenance contacts and support plans (maintenance windows, communication pathways for downtime announcements, etc.)
- Business Continuity Plan which identifies how clinical users will continue to deliver services in the case of an outage
- Backup and Disaster Recovery plans including measures for RTO (Recovery Time Objective), MTO (Maximum Tolerable Outage), and RPO (Recovery Point Objective)
- End user support plans (if applicable) and administrative/operational support plans
- Operational Contingency Plans
- Service desk and official communication information

6.2.7 Authentication

Services which comprise the DHP should require the use of authentication context sharing to perform duties between their services. It is expected that all services in the DHP will accept and appropriately use identity assertions via a bearer token infrastructure (or appropriate session token shared with in messages of other formats such as the MSH-8 of HL7v2 traffic).

As per IETF RFC 6750[131] "...any party in possession of a bearer token "(a "bearer") can use it to get access to the associated resources (without demonstrating

[131] https://datatracker.ietf.org/doc/html/rfc6750

possession of a cryptographic key). To prevent misuse, bearer tokens need to be protected from disclosure in storage and in transport."

The DHP should provide a centralised identity provider which allows PoS applications integrating with the DHP to obtain access tokens for message passing. This will require authentication of applications (via a valid client identity and client secret) and assertion of a user identity. The identity provider shall produce for the point of service application:

- An access token which relates to the session established for the transaction with the DHP including:
  - Access grants (scopes)
  - The identity of the bearer (application or user)
  - The intended audience of the token
  - The expiration (not after) time
- An identity token which includes structured information about the security principal including:
  - The issuing identity provider
  - Issuance time and expiration time (not before and not after)
  - The name, e-mail, and telephone number of the user
  - The identity of the application which was authenticated
- A refresh token which should be used to extend the session

All DHP services are expected to validate the access token with the identity provider from which the token was issued. The access tokens and identity tokens should be digitally signed by the identity provider so that DHP services can verify the authenticity of the access token.

The authentication of device nodes is best practice between point of service applications and the NHDX. This authentication should be used to validate that:

- The software on the device and the device itself has:
  - A proper security environment established
  - Standards interfaces have been properly implemented and validated (passed conformance testing)
  - Appropriate business processes have been put in place at the PoS location
- The device from which the request originates is trusted within the enterprise
- The device from which the request originates has not been revoked or failed re-validation after expiration of access credentials.
- The device from which the request is made is using TLS

Typically, these layers of security are implemented using dual-PKI (public key infrastructure) certificates for node authentication[132], and OpenID Connect for application and user authentication[133].

6.2.8 Authorisation

The authorisation of security principals to application functions within the services of the DHP is expected to be highly specific to the use case and service (example: a client registry will have different authorisation requirements than the national EHR). The authentication token and authorisation of that token to scopes will be performed centrally in the identity provider for the DHP (emitting permitted scopes of access).

The enforcement of these directives/authorisation is to be handled by the DHP service rather than centrally. This allows each service to identify and handle appropriate enforcement methods including:

[132] IHE ITI TF Vol2 – ITI-19 Authenticate Node

[133] OPENID Authentication Flows (hidglobal.com)

- Masking, redacting, or removing sensitive data
- Rejecting or blocking actions
- Elevating or flagging audits
- Notifying relevant security personnel

6.2.9 Auditing and Accountability Tracing

All DHP services which provide a functionality to the DHP, or which consume data from the DHP are required to keep a structured audit trail[134]. This audit trail must be validated before integration with the DHP, and it must contain, at a minimum:

- The nature of the audit event (login, create, delete, etc.)
- The standardised trigger event which was executed (create discharge summary, refer patient, etc.)
- The full date and time that the event occurred
- The actors who were involved in the interchange including:
  - Identification of the source machine (which initiated the interchange)
  - Identification of the target machine (the recipient of the interchange)
  - Identification of the human user (if appropriate)
  - Identification of the process name, classification, etc.
- A list of all objects which were created, modified, disclosed including:
  - Identification of the object which was impacted
  - The type of the object (user, patient, document, etc.)
  - The nature of the data lifecycle for the object (amended, disclosed, deidentified, etc.)
- The query executed (if appropriate) including:
  - The query parameters which were used to search the service

Each trigger event definition in the logical view will identify specific audit requirements of the producer and consumer including:

- Trigger event identifiers
- Objects expected to be in the audit
- The roles and codes of the actors involved

Security audits shall be performed on all information systems before connecting to the DHP (i.e. prior to issuance of a device or application credential for DHP access)[135],[136].

6.2.10 Informational Consent Directives

The DHP will store sensitive personal health information (PHI) and it is important that the directives related to the disclosure or use of this PHI be stored in a fashion which identifies clear directives by the patient for the use of this data. The consent directive service in the DHP is a repository which will be used to store documentation (or directives) of the patient in relation to the use of their data in the DHP. XML Access Control Markup Language (XACML)[137] architecture components should be used as a framework for enforcement of consent directives within the DHP. The architecture is summarised in Figure 38:

[134] National Digital Health Guidelines and Standards [2] Section 6.3.3

[135] National Digital Health Guidelines and Standards [2] Section 3.1.10

[136] National Digital Health Guidelines and Standards [2] Section 6.3.12

[137] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

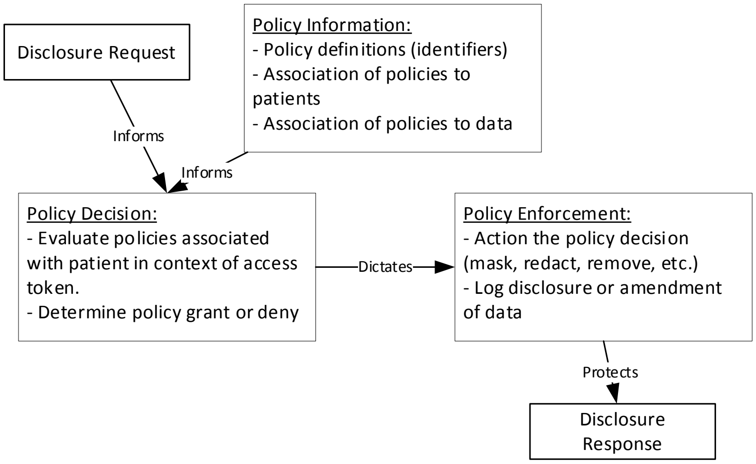

Disclosure Request
Policy Information:
- Policy definitions (identifiers)
- Association of policies to patients
- Association of policies to data
Informs
Informs
Policy Decision:
- Evaluate policies associated with patient in context of access token.
- Determine policy grant or deny
Dictates
Policy Enforcement:
- Action the policy decision (mask, redact, remove, etc.)
- Log disclosure or amendment of data
Protects
Disclosure Response

Figure 38 : *Policy Information, Decision and Enforcement*

- Policy Information: Data and security tags which are used to identify which policies exist, their definition, and to which object these policies apply.
- Policy Decision: Performed by the identity provider to establish a list of scopes for an access session using policy information tagged on the identity provider source.
- Policy Enforcement: Performed by the DHP service (such as client registry, NEHR, etc.) to take context appropriate action. Actions could include:
  - Masking data which is sensitive (i.e., modifying HIV ART numbers)
  - Removal of sensitive data
  - Disclosure of sensitive data with additional auditing
  - Alerting of appropriate authorities

This framework should also be used by administrators reviewing data exports for non-health delivery use cases such as research, justice system investigations, etc.

6.2.11 Transaction and Message Control

The DHP must provide reliable delivery, retry, error handling, queueing, and acknowledgement functions regardless of whether the transaction is pass-through or orchestrated.

To support this function, all messages submitted to the DHP must contain in appropriate message wrappers (HTTP headers, FHIR Provenance and MessageHeader resources, etc.) which contain:

- The originating organisation and facility
- The application instance which generated the information (e.g., HHIMS running at Dompe Hospital)
- Transaction and trigger event identifiers
- The patient or subject(s) of care to which the message applies
- The author(s) (i.e., who captured the data and prepared it)
- The data enterer where appropriate (i.e., who transcribed the data into the computer)
- The performer(s) where appropriate (i.e., who performed the medical intervention)
- Authenticator (i.e., who signed the data as being accurate)

- An assertion of the user who interacted with the EMR to create and send the message

Messages received by the DHP should be considered transient data structures. The payloads of these structures are to be extracted and persisted as appropriate, however persistence of the entire messages themselves is discouraged (beyond functions for retry or audit).

6.2.12 Error Handling and Retry

The DHP uses a service-oriented architecture whereby services are orchestrated and/or composed to solve a particular business problem. This architecture, while flexible, presents a challenge when handling errors as there are multiple tiers in which errors could occur.

Consider, for example, a point of service (PoS) contacting the DHP to post a document to the NHDX. Such a transaction from the point of view of the PoS is opaque, however the DHP would rely on the orchestration of several services to achieve the business goal (illustrated in Figure 39).

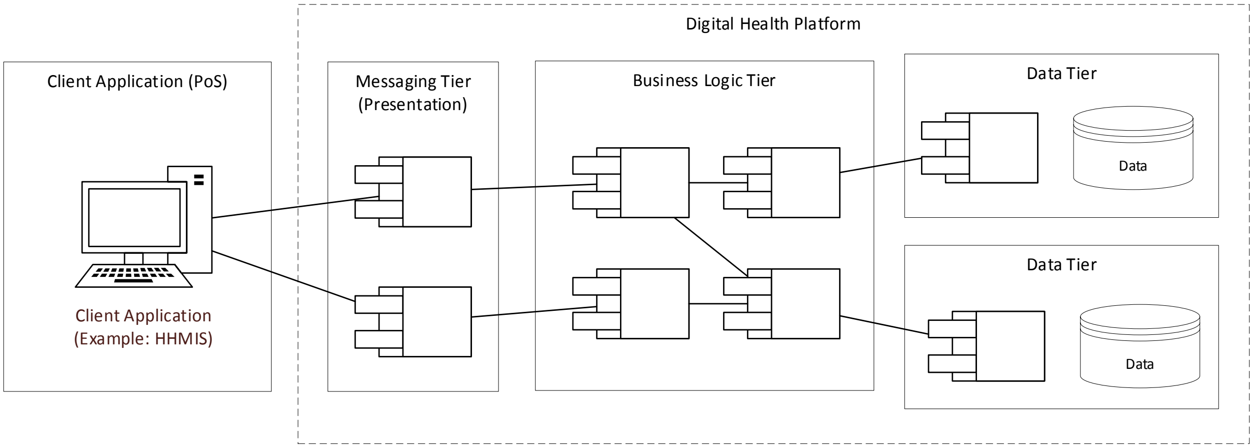


Figure 39 : *Service Orchestration and Composition in the DHP*

Because these services in the DHP are independent units of functionality, any number of errors may arise:

- Data / Business Errors: Issues related to incorrect data or incorrect business processes including:
  - Nonsensical data submitted (i.e., last menstrual period observation for a Male patient)
  - Incorrect procedure or battery codes (i.e., incorrect specimen collected for requested test)
  - Business process codes (i.e., submitting a lab result for an order which does not exist)

Business errors typically require user intervention to correct and require the PoS to alert the user and capture new data.

- Infrastructure Errors: Issues related to the physical environment on which the service is running including:
  - Network issues
  - Server faults
  - Power grid failures
  - Update or Operating System configuration issues

Infrastructure errors can typically be resolved automatically by retrying the operation after the underlying issue has been corrected.

- Application Errors: Issues related to the application logic of the service itself including:
    - Incorrect implementation of application logic
    - Incorrect understanding of messages sent to the service
    - Database consistency issues

Application errors typically require an update to the business logic, or service code to correct and can typically be corrected with a retry once the application is updated.

- DHP Errors: Issues with the completion of the operation because of logical errors within the context of the entire digital health platform including:
    - Inability to resolve necessary information
    - Security issues such as access rights or permissions issues
    - Missing or incomplete service problems

DHP errors may require further investigation into the cause of the issue and may require manual intervention by an administrator or data quality personnel.

Whenever a DHP service encounters any of these types of errors, it is important that this feedback be relayed to the PoS application which invoked the service. The DHP service component and DHP should relay errors to the PoS application in a structured form with as much detail as possible (rather than an unstructured exception handling page).

The structure of the exception will vary depending on the standard used to initiate the interchange (for example: FHIR interfaces should use the Operation Outcome[138] resource). Whatever the format of the exchange, the exception structure should contain:

- A system error code which allows for a computable method of resolution (for example: PostgreSQL error code, stop code, etc.)
- An indication of the severity of the exception:
    - Information: The transaction was processed by the component of the DHP successfully, however there is contextual information for the end user about the transaction (for example: Patient ID has been replaced with new ID)
    - Warning: The transaction was processed successfully, however there may have been some modifications to the way the transaction occurred. (For example: ICD9 code X has been retired, use ICD10 code Y)
    - Error: The transaction could not be processed successfully. There was a business, infrastructure, application or DHP error which prevents the operation from completing.
- Underlying cause of the exception in structured form. The exception result will have a primary issue (example: Record could not be found) with an underlying cause (example: Could not resolve patient information) which itself may have a further cause (example: Database is Offline).

After relaying this information to the PoS system, the solution must decide on appropriate action which could include:

- Re-submitting the errored request later automatically
- Display an error message to the user requiring a correction
- Notifying a system administrator of the issue

[138] OperationOutcome - FHIR v4.3.0 (hl7.org)

Implementations of DHP services should ensure that exceptions are raised at the appropriate tier, as close to the exceptional cause as possible, and should include relevant codification of the issue and its severity on the transactional processing of the request.

If possible, exceptions should "bubble"[139] through the DHP service layers and should halt processing (i.e., an exception in the Client Registry should stop processing in the business logic tier, then via the integration tier back to the PoS). If using asynchronous processing of messages such as in the case of an Enterprise Service Bus[140] (ESB), it is expected that the integration layer (the NHDX) persists information about the exception it has received from a service.

[139] Implementing Exceptions in SOA (infoq.com)

[140] Erl, Thomas. SOA Design Patterns. Pearson Education, 2008. Pg 704-706.

7.

Realising the Blueprint

The blueprint described in this document provides a framework and guidelines for digital health system design and decision making. It describes the overall shape, structure, and methodology of the development of the national digital health infostructure for Sri Lanka. This section is intended to provide guidance on getting started on realising the Blueprint, moving from Blueprint to project planning and eventually to implementations.

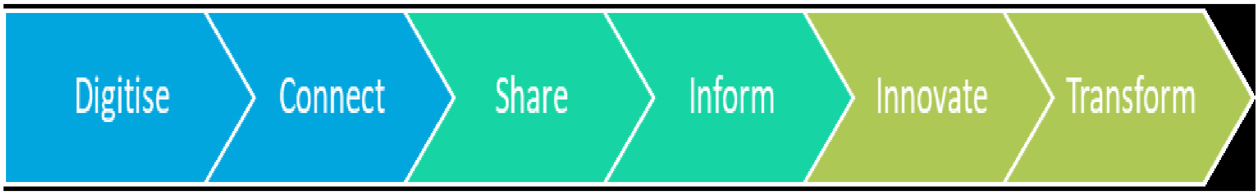
This section will identify the stages of evolution that will be encountered and identifies some of the core building blocks and activities that can be started right away. It also provides a map of the dependencies between the major blueprint components to be realised on the way to the full digital health environment and provides concrete next steps forward in the Prioritised Action Plan.

The goals of the Blueprint are to build upon what has already been accomplished in Sri Lanka with previous investments by incorporating existing systems wherever possible and designing for future reuse. It is expected that the implementation of the Blueprint will not be done as a single large project, rather it will be developed incrementally over time as resources become available.

The Blueprint presented in this document has also been designed to be "future-proof", in the sense that it is flexible enough to support new priorities for health care service delivery and to be able to reflect new digital health functional opportunities. The approach described here will align with and enable health system transformation to guide digital health investments over the long term.

7.1 Stages of Evolution

The recommended approach to realising the Blueprint is summarized as six broad stages[141] of evolution in the following diagram:



These generalized stages are discussed in the following section, and a more specific prioritised action plan follows thereafter.

7.1.1 Digitising Clinical Information

The first stage of evolution is to begin the process of workflow digitisation, wherever and whenever possible. As part of this process, patient journeys, clinical workflows, etc. will need to be optimized and streamlined, as proceeding with digitising inefficient workflows will reinforce bottlenecks that poorly impact delivery of services. Digitisation in this context is defined as adapting a system or process to make use of digital devices and networks. This can mean introducing and/or expanding the use of digital devices and systems, electronic forms, and data capture throughout administrative and clinical processes. This is also the first step to workforce capacity building through digital literacy and involves on-boarding as many users as possible to utilise digital technologies in the clinical and administrative environments on a daily basis.

7.1.2 Connecting Digitised Solutions

The next (or if possible, in parallel) stage of digital evolution is to begin to connect people, institutions, facilities, and systems across the health enterprise. Secure, reliable connectivity and centralised authentication, authorisation and communications systems are a fundamental requirement to move towards a more advanced digital ecosystem. Connectivity and security should begin with care providers and administrators, then be extended continuously further out to patients/clients and clinicians in the extended circle of care, as well as organisations such as licensing bodies and government departments as required. While the fundamental connectivity and security is being rolled out, design and development of the shared health services components of the digital health platform should be underway.

7.1.3 Sharing Clinical Information

Once digital workflows and connectivity are in place, the process of sharing will begin to happen naturally. Both structured processes and ad hoc communications will occur using clinical applications and communications tools as providers consult with each other and ultimately with patients. Sharing will eventually evolve to using more advanced clinical applications as components of the digital health platform are developed. For example, once key registries and subsystems are in place, development of advanced applications such as eReferral can begin.

7.1.4 Informing Health Decisions

Once systems and applications are digitally connected, and information repositories are created and can share information, users will be able to interact with new levels of structured information, allowing them to incorporate information and evidence that supports informed clinical decision making. For example, an advanced

[141] Adapted from: Parker, Ron. Enabling Coordinated and Collaborative Health Care. Canada Health Infoway, 30 March 2016. Webinar.

national vaccination forecasting application can make use of immunization data collected by other applications such as EMRs. Through the use of standardized data structures and terminologies, applications can share and make use of clinical information collected from other sources.

7.1.5 Clinical Innovation

A fully realised platform with connectivity, structured interoperable data and clinical intelligence forms the platform to begin to innovate and support patients or consumers to improve their own health using advanced, specialised applications and tools, while also enabling clinicians to provide better care.

For example, one innovation currently under development by WHO are Computable Care Guidelines (CCG) which helps close the chasm between what we know are the evidence-based best practices and what is done for individual patients. CCGs provide a standards-based way to describe and to share the minimum data set that should be collected during an encounter, the workflow that is to be triggered based on collected content as well as the reportable health system management indicators that may be automatically generated from the encounter.

Importantly, CCGs provide us with a mechanism to track and monitor care delivery activities. The innovative digital health solutions created on the platform provide person-centric context based on the CCG's dataset, and these support care continuity and quality assurance and support a future culture of patient-centred care.

As stated by Robert Kish[142], "an engaged patient is the blockbuster drug of the century".

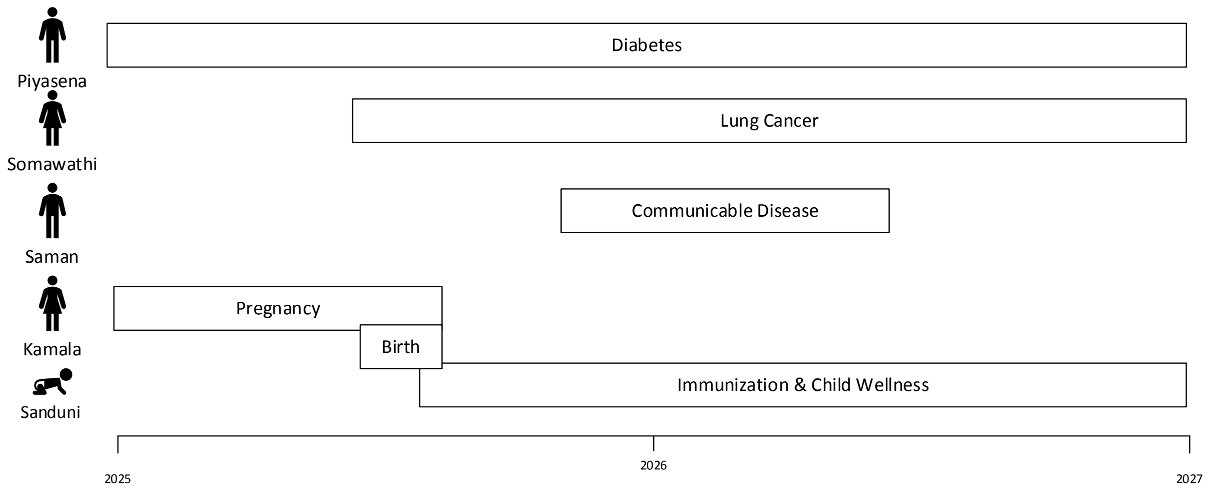
7.1.6 Digital Transformation

Finally, a fully realised platform will provide the information and analytics to enable data-driven decision making and give administrators the ability to truly transform the health system. It should be noted that the development of a national digital health platform is not a single top-down construction project, rather it is an iterative and incremental activity that evolves to support high priority Patient Journeys. The digital health platform is designed to be developed and deployed as resources become available, growing organically as more infrastructure and components are built and as more external applications are connected. As implementations mature, specifications will evolve, functionality will grow, and the health system of Sri Lanka will begin to transform.

7.2 Patient Journey Stories

The blueprint will be realized in the context of user stories which following the life of a fictional Sri Lankan family as they interact with the health system across Sri Lanka. These stories represent typical user journeys that a Sri Lankan family might take as they interact with the different programmes, and health facilities during their lifetime. The family consists of 5 members, who interact with a potential future state DHP deployed in Sri Lanka.

[142] Kish, L. (2012) The Blockbuster Drug of the Century: An Engaged Patient. HL7 Standards. http://www.hl7standards.com/blog/2012/08/28/drug-of-the-century/



These stories are used as the basis for realizing the blueprint in a phased manner, and comprise of clinical events related to:

- Non-communicable diseases such as diabetes and cancer illustrating the care of a patient as they visit a variety of health centres for a variety of treatments over time,
- Communicable diseases such as TB, dengue, COVID which result in a series of treatments and diagnostic procedures requiring cross agency participation with preventative and curative sectors,
- Pregnancy and birth and childcard which result in new registrations of persons in Sri Lanka linked to one another and cases with children who lack National Identity Cards (NIC).

The stories illustrate the cross-system use of the DHP, while allowing blueprint implementation to be expressed in terms of patient use and clinical outcomes.

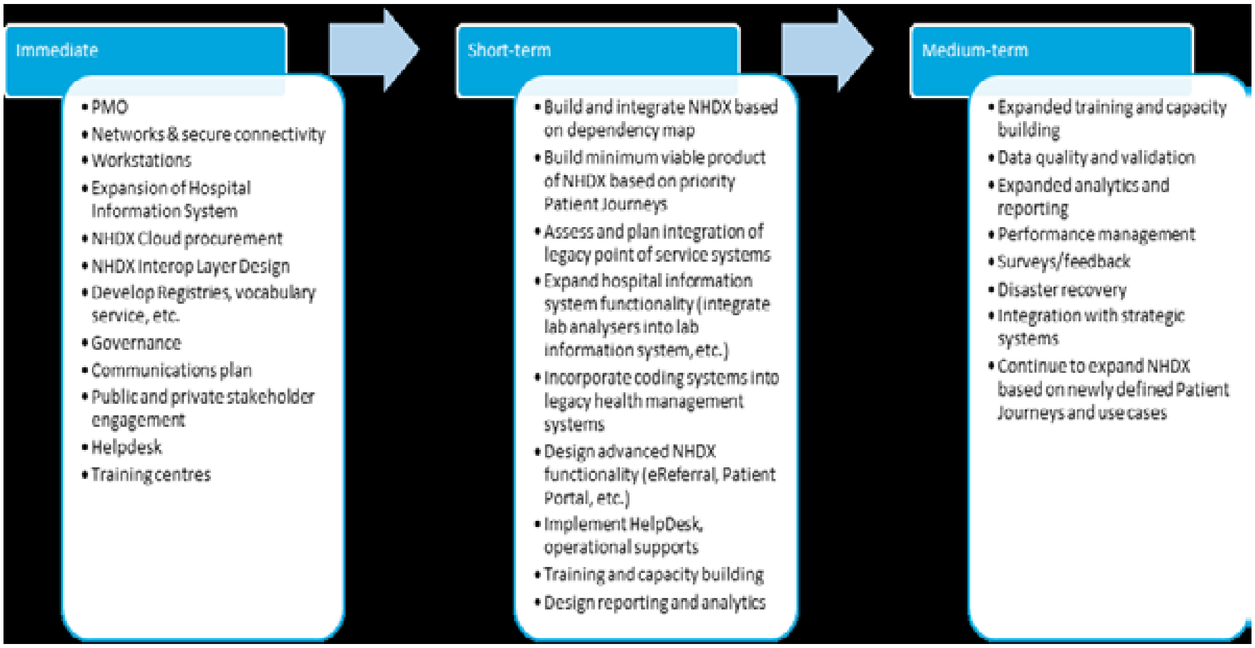
7.3 Blueprint Implementation Roadmap

The Blueprint is a conceptual architecture document which provides a high-level conceptual view of the future state of the proposed digital health platform. Although this section provides some actions that should be taken towards realisation, the Blueprint is not intended to be a detailed project plan or roadmap.

Additional considerations from the other design artefacts for the digital health transformation will be described in a separate roadmap document including:

- Considerations for interoperability profile development and component specifications
- Considerations for procurement of physical hardware and software
- Considerations for onboarding experts and human resources

The roadmap will set out objectives and timelines including dependencies, milestones, deliverables, and responsible persons for the implementation and realisation of the blueprint and its component pieces. The high level activities for the realisation of the digital health blueprint is illustrated in Figure 40.



Immediate

- PMO
- Networks & secure connectivity
- Workstations
- Expansion of Hospital Information System
- NHDX Cloud procurement
- NHDX Interop Layer Design
- Develop Registries, vocabulary service, etc.
- Governance
- Communications plan
- Public and private stakeholder engagement
- Helpdesk
- Training centres

Short-term

- Build and integrate NHDX based on dependency map
- Build minimum viable product of NHDX based on priority Patient Journeys
- Assess and plan integration of legacy point of service systems
- Expand hospital information system functionality (integrate lab analysers into lab information system, etc.)
- Incorporate coding systems into legacy health management systems
- Design advanced NHDX functionality (eReferral, Patient Portal, etc.)
- Implement HelpDesk, operational supports
- Training and capacity building
- Design reporting and analytics

Medium-term

- Expanded training and capacity building
- Data quality and validation
- Expanded analytics and reporting
- Performance management
- Surveys/feedback
- Disaster recovery
- Integration with strategic systems
- Continue to expand NHDX based on newly defined Patient Journeys and use cases

Figure 40 : *High Level Roadmap*

The roadmap will be developed by selecting a series of patient journeys which are of key strategic importance to the MOH. These journeys are used to derive a minimum set of components which can be implemented related to the blueprint over time.

From the roadmap, workpages will be developed which may occur in parallel to increase the velocity of realisation of the blueprint components. Regardless of the specific user journeys selected for implementation, common blueprint components have been identified for initial implementation:

- Establishment of a common PMO, finalisation of documents and plans,
- Digitisation of points of service applications so they may contribute and consume data to/from the DHP,
- Key infrastructure including underlying infrastructure (compute and network resources)
- Implementation of security services identified in the blueprint (certificate services, audit, time keeping, etc.),
- Integration services contained within the NHDX (messaging, API management, etc.),.
- Registries which facilitate the consistent and authoritative identification of resources used within the digital health platform (client registry, provider registry, institution registry, terminology services).

The remainder of services in the blueprint can then be additively implemented within the blueprint over time as patient journeys are documented and prioritised for implementation.

The blueprint realisation roadmap document further describes the phases of realisation and implementaiton.

7.3.1 Existing Project Alignment

At the time of this writing, the Ministry of Health Sri Lanka is currently undertaking several major projects for the enhancement of digital health systems, workforce enhancement and aggregate and reporting systems. These projects include an upgrade of the Hospital Health Information Management System (HHIMS), a wide scale deployment of OpenMRS, and the implementation of an upcoming drug management information system called "suwatpetha".

These projects will begin alignment to the blueprint via adoption of common blueprint principles.

The largest portion of current project activities involve digitisation of health records within the HHIMS, expanding infrastructure and connectivity, and sharing of information a subset of use cases between points of service. The focus on these activities primarily resides within an upgrading and implementation of HHIMS which is a point of service solution within the DHP. This work is being aligned with blueprint functional principles and services and provides an impactful starting point to realising the blueprint for broader use cases.

Other activities being undertaken focus on the establishment of registries, harmonising terminology, and the profiling and definition of APIs into the digital health blueprint. These activities are an opportunity for implementing the required dependent blueprint assets within the scope of a concrete problem being solved. For example, a desire to implement e-Referrals between HIMS, HHIMS and the cloud based HIMS would require the implementation of blueprint services (see section 7.4.1).

Included below is a summary of project activities which have been identified as strategic by the MOH:

- Digitise
    a. Personnel Recruitment Activities
        i. Hiring of developers, architects, managers, etc. to scale-up necessary talent (recruitment) via ICTA
        ii. Establishment of a Programme Management Office
    b. Improvements to the Hospital Health Information Management System (HHIMS)
        i. Procurement of workstation hardware for registration clerks, clinicians, nurses' stations, radiology workstations and related networking equipment
        ii. Procurement of localised server infrastructure required for hospital hosting of data and functions
        iii. Integration between the lab module (LIS) and existing analyser equipment
        iv. Establishing business continuity and disaster recovery plans for updated HHIMS
    c. Harmonisation of Digital Records
        i. Establishing common terminology for use within digital health solutions using standardised code sets (such as ICPC-2 and ICD-10 coding systems)
        ii. Enhancing governance of hospital and digital health solutions via Standard Operating Procedures (SOPS) and procurement plans for hospitals.
    d. Strengthen Digital Health literacy
        i. Design training modules for trainer of trainer scenarios related to the hospital information management upgrade including ICD10 and ICPC2 coding.
        ii. Train HIU staff on integration between existing modules for health intervention (such as DHIS2) and the central infrastructure
        iii. Train frontline hospital health staff on basic ICT literacy and hospital information systems processes/ workflows.
    e. Measuring the Impact of Digital Medical Records
        i. Create a data validation methodology to ensure digital health solutions are being appropriately used.
        ii. Measure the satisfaction of primary and secondary care digital health systems (clinicians and administrators)

to develop and validate SOPs and guidelines

- Connect
  a. Establish connectivity for clinics and hospitals with each other and with central infrastructure using 4G / 5G
  b. Establish a National Help Desk and related functions (starting with HHIMS use cases and SOPs)
- Share
  a. Establish common registries required for the operation of health information systems in Sri Lanka (focus on Hospital Health Information Management System - HHIMS)
  b. Establish integration strategy for SLUID
  c. Establish / Pilot an e-referral solution leveraging the blueprint infrastructure (example: between OPD and hospital systems)
  d. Establish / Define standards-based APIs and integration profiles in line with the blueprint between private sector and public sector institutions to the national level.
  e. Develop / Pilot the integration of information from disease program information systems with HHIMS using the NHDX and/or NEHR functionality.
  f. Establish a public reporting pathway whereby select statistics can be published on the Ministry of Health Website (starting with primary care morbidity data)

This list is not an exhaustive plan for blueprint realisation. Such realisation may take more than a decade to fully complete. The blueprint will serve as a guidepost for future activities, funding requests and investment in digital health interventions within Sri Lanka (see section 2.5.7).

7.3.2 Interoperability Plan

As detailed in the blueprint (section 2.3.2 on page 27), each service will require the further definition of transactions, trigger events, and domain specific interoperability profiles for implementation. The order in which these solution and technical views will be developed will be detailed in the companion Interoperability Plan document.

This process will require inputs from multiple stakeholders across various groups in the the MOH, ICTA, private vendors, and operators. The Interoperability Plan is a separate document which accompanies the blueprint and describes:

- The governance of standards and interoperability adoption in Sri Lanka
- The processes used to adapt and measure conformance to standards
- Cross-standards guidance to be considered when implementing and using interoperability profiles
- An initial series of interoperability profiles which need to be adapted for Sri Lanka.

7.4 Blueprint Dependency Map

Regardless of the maturity of the end-state functionality, key infrastructure components must be in place for any digital health platform to function. This is like requiring power and water plants built before housing and apartments in a city.

The realisation of the blueprint into the full DHP may take a decade or more to complete, and rarely does such a complex task occur in one single, large project. Rather, the implementation of the blueprint will evolve through independent projects, each leveraging or requiring portions of the digital health platform to solve concrete digital health problems.

Figure 41 provides an overall dependency mapping of the entire blueprint systems architecture. The diagram illustrates how each service to be implemented in the blueprint depends on other services and is intended to provide an informative guide to understand the order of operations of implementation. The diagram is simplified for illustrative purposes and does not show direct dependencies.

For example, a project which requires the use of the Master Patient Index would require implementation of the NHDX, an Identity Provider, Timekeeper, and an Audit Repository. The dependency between Master Patient Index and Identity Provider is not explicitly illustrated because the dependency of the NHDX by the MPI indicates this.

While the diagram establishes an overall dependency tree, the reader should be mindful that an indication of a dependency may not represent an entire implementation of the dependent service, rather only a subset of functionality for that service may be required. Like the DHP itself, each service may have its independent lifecycle and evolution.

For example, the establishment of an identity provider (IdP) may require certificate services, however only the functionality of certificate services as defined in section 4.2.7.2 sufficient to support the IdP are required.

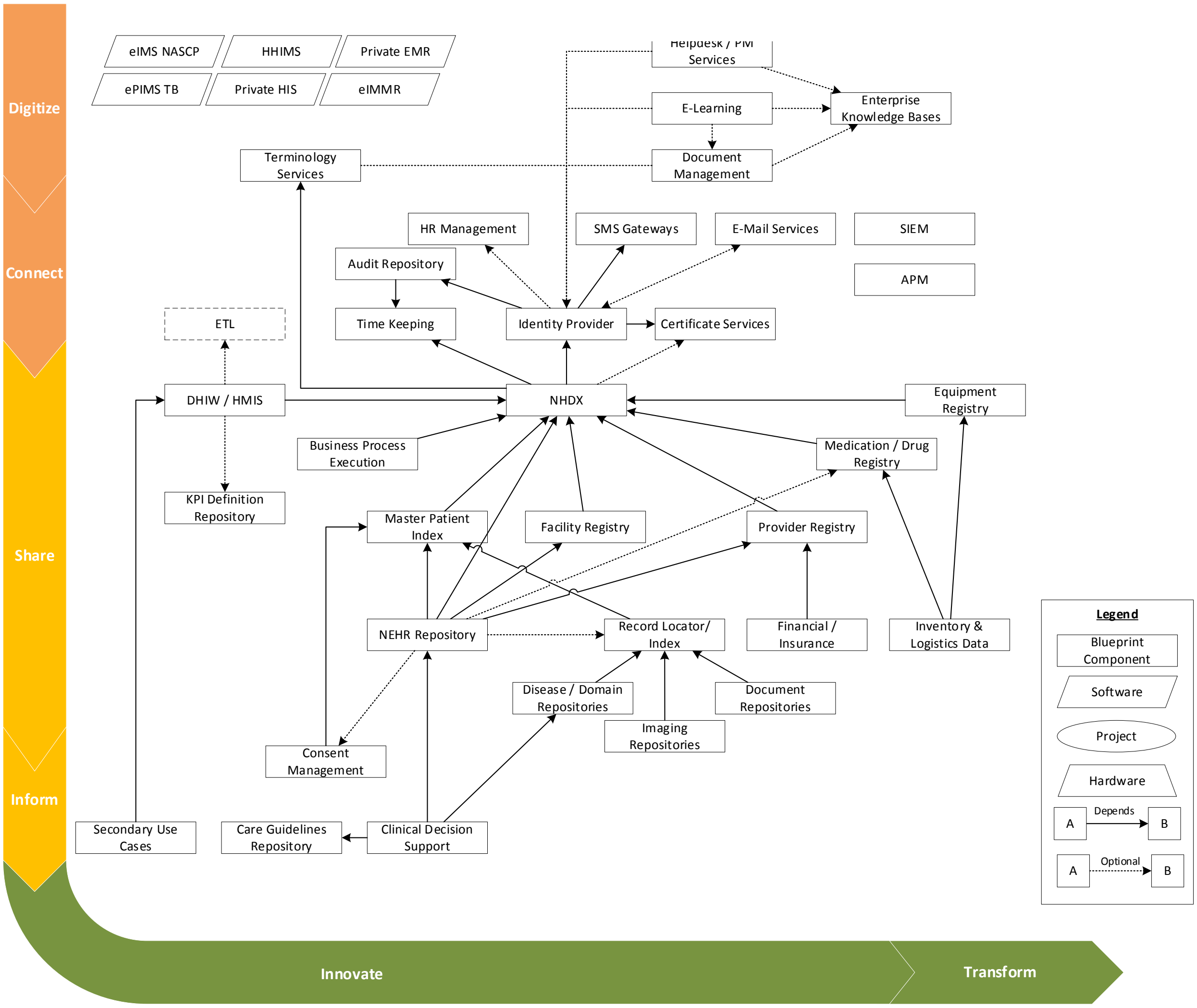


Figure 41 : *Blueprint Component Dependencies*

The complete dependency list between blueprint components is enumerated in **Error! Reference Source not found.**

7.4.1 Dependency Map for Diabetes Patient Journey

The initial implementation of the DHP will involve a patient journey using Piyasena through his diabetes care. During this encounter, he receives care at Pugoda Primary Care Unit, is referred to Dompe Divisional Hospital, receives an amputation at NHSL, and receives post-surgical care at Gampaha district general hospital surgical and medical clinic.

The dependency map included in the blueprint can then be used to establish which components of the blueprint need to be implemented first to support this use case as illustrated in Figure 42.

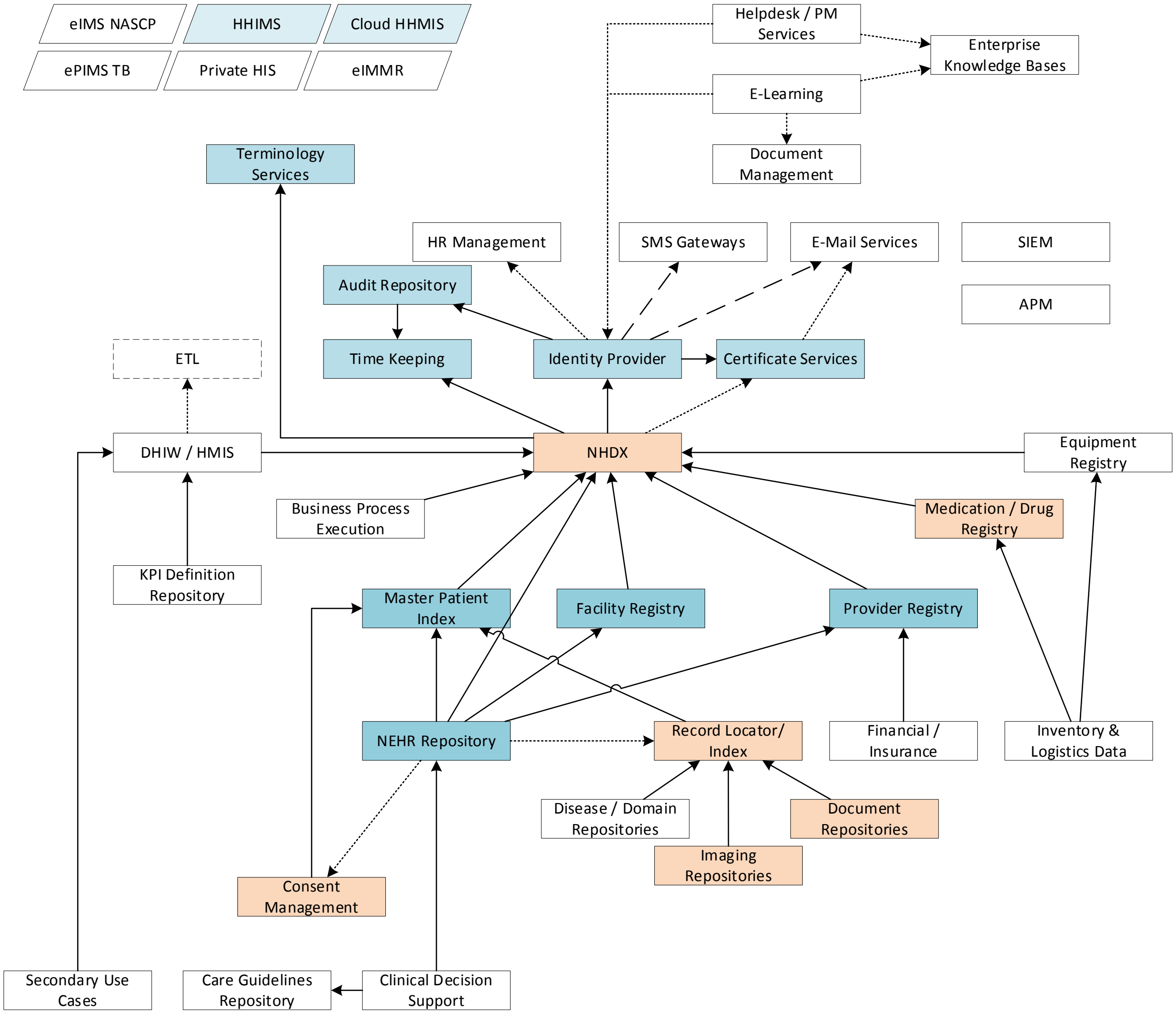


Figure 42 : *Diabetes Project Dependency Map*

7.5 System Implementation

When implementing specific components or systems, there are essentially four approaches for obtaining software to satisfy the system requirements collected during the design phases described above.

The preferred approach is to adopt common off the shelf (COTS) software (open source, or commercial) and applying configurations and extensions to perform the desired function. If adoption of software is not possible, the adaptation of existing open source solutions in a frugal manner should be attempted before commencing a "from scratch" custom software. This approach is often labelled adopt, adapt, develop.

7.6 Operating Environments

In a complex enterprise such as a national digital health system, several system operating environments are normally established. The blueprint proposes that four working environments be established for the DHP and its components:

- *Development:* Established primarily for the purpose of developing new functions
- *Testing:* Established for the purpose of testing components, performing quality assurance and conformance and compliance validation with synthetic data.
- *Staging:* A configuration which mimics the production environment and is populated with anonymized copies of data for the purposes of training, issue resolution, and final pre-production validation. The staging environment's configuration should closely match that of the production environment.
- *Production:* Containing the actual personal health information and components operating in a "live" environment and is substantially larger than the other environments and implement much more stringent security, monitoring, redundancy, and scaling configurations.

7.6.1 Strategic Environments

Beyond the various environments used for the ICT operations lifecycle, many jurisdictions have created additional environments for strategic purposes. Two such examples are:

- *Reference Implementations:* A software package or system that implements the detailed specifications for new standards, components, which serve as a reference for implementers to understand how software solutions in the broader DHP will interact.
- *Sandbox Environment:* An open environment with less stringent access requirements that mimics the actual production environment in its features with fake, but exemplary data. The sandbox is used to showcase the functionality of the DHP to the broader public and allow software developers and users to explore and innovate on the technologies implemented.

Annex A - Directorates of the Line Ministry of Health

This section provides a summary of the Deputy Director Generals within the Line Ministry of Health and their directorates, for the reference of the reader.

DDG	Directorates
DDG Finance I	• Expenditures (Directors of Expenditure I – III) • Coordination (Director Ca & Cord) • Bookkeeping • Supplies Management
DDG Finance II	• Budgeting • Stock Verification
DDG Public Health Services I	• Epidemiology • Quarantine • Disease Monitoring (Dengue CU, NSACP, etc.)
DDG Public Health Services II	• Maternal & Child Health • Nutrition • Public Health Nursing
DDG Medical Services I	• Private Sector Development • Mental Health Services • Nursing
DDG Medical Services II	• Primary Care Services • Hospital & Acute Care Services
DDG Planning	• Planning Services • Organization Development • Health Information Services • International Health Reporting • Policy Development and Analysis
DDG Education, Training	• Training & Recruitment • Nursing Education
DDG Dental Health	• Dental Services
DDG Building & Logistics	• Engineering and Building Services • Building & Facility Administration

Annex B - Current State Assessments Reviewed

Stakeholder groups completed a PowerPoint template which was used for prompting feedback. The results of these were analysed and common traits/requirements of these stakeholder groups and their systems are shown in Table 3.

The stakeholder groups for which there was a current state assessment performed prior to the authoring of the blueprint were:

- DDG Management Development and Planning Unit
- DDG Medical Services Unit I
- DDG Medical Services Unit II
- DDG PHS 1
- DDG PHS 11
- DDG Laboratory
- DDG dental services (pending)
- DDG bio medical (pending)
- DDG NCD
- DDG medical supplies
- Family health bureau
- Health Promotion Bureau
- Epidemiology unit
- Nutrition coordination unit
- Quarantine Unit
- Anti-Leprosy Campaign
- National Programme for TB and Chest Disease (NPTCCD)
- National Dengue Control Unit
- Antimalaria Campaign
- National STD and AIDS Control Programme (NSACP)
- HHIMS Project (Architecture Review)

Additional stakeholder groups interviewed after the initial development of the blueprint are not included in this list.

The assessment attributes are labelled using X where the current digital health solutions match this attribute, P when the attribute has been planned, and I where explicit descriptions of the functionality is not provided rather, it is inferred.

Table 3 - Common Attributes of Current State Assessments

	Anti-Leprosy Campaign	Health Promotion Bureau	Quarantine Unit	TB and Chest Diseases	National Dengue Control	Antimalaria Campaign	HHIMS (Architecture)	NSACP	Medical Services I & II	Planning Unit
Register and track Patient Demographic Information for contact and follow-up.	X		X	X	X	X	X	X	X	
Register and track discrete patient health care event data.	X			X	X	X	X	X	X	
Patient Centric Design	X		X	X			X			
Case Centric Design						X				
Track geographic location of patient for communicable disease tracing	P			X	P					
Provides central level tracing of patient events and sharing between providers in different geographic regions.	X			X	X		X			
Provides business-unit decision support services related to follow-up, care planning, etc.	X			X	X		X			
Enforce data level security to ensure patient privacy is protected (i.e., protect data from inappropriate disclosure or access based on role or policy).	P			X						
Enforce system level security to ensure only authorised users are permitted to access system functions (i.e., username and password).	X	X	X	X	X	X	X	X	X	
Generate aggregate indicators for preparing management reports.	X	X	X	X	X		X	X	X	
Used by clinicians while providing care. The solution guides physicians in the execution of their duties (rather than being used as a documentation only system after the care encounter has completed).				X	X		X	X		
Used by administrative users (or non-clinicians) to input aggregated or administrative data (rather than discrete clinical data events)	X	X				X				
Generates comparative data with different reporting periods (provides the basis for comparative indicators)	X		X	X			X			

	Anti-Leprosy Campaign	Health Promotion Bureau	Quarantine Unit	TB and Chest Diseases	National Dengue Control	Antimalaria Campaign	HHIMS (Architecture)	NSACP	Medical Services I & II	Planning Unit
Adheres with NDHGS standards for data capture or exchange.	X			I			I			
Accessible from different clinics, locations and communicates with central infrastructure (i.e., within the system patient data flows between clinics).	X	X		X	X	I	X	X		
Monitor the work of medical officers, nurses, or other providers in their daily duties (i.e., assign work schedules, duty assignments, etc.)		X					X		X	
Engage, disseminate, and monitor health activities directly with patients. Patients are provided tools for interacting with digital health systems.		X	X							
Disseminate and collect information to/from public health workers/officers for the monitoring of public health concerns (communicable diseases, quarantine, etc.)		X	X				X			
Mission critical infrastructure/solution (i.e., business processes are digitized, and outages directly affect daily duties of users)	X	X			X	X	X		X	
Share data across different software solutions to promote monitoring of health system and related activities (campaigns, outreach, etc.)	I	I		X	P					
Monitors the public health status of foreigners and non-citizens.			X							
Monitor the public health status (tests, communicable disease status, vaccination, contacts, etc.) of citizens.			X	X		X	X	X		
Require disclosure/conveyance of individual events over time of care of client or encounter with client (individual observations, procedures, etc.)	X			X	X		X	X		
Require disclosure/conveyance of data in a document form (discharge summary, referral note, radiology notes, etc.)			X				X			

	Anti-Leprosy Campaign	Health Promotion Bureau	Quarantine Unit	TB and Chest Diseases	National Dengue Control	Antimalaria Campaign	HHIMS (Architecture)	NSACP	Medical Services I & II	Planning Unit
Track the status, delivery, and consumption of consumables/stock/supplies.				X	P	X	I			
Integrate data exchange with laboratory systems for diagnosis, specimen collection/registration, and result view.						P	X	X		
Integrate/track digital diagnostic imaging source images and/or PACS solutions.				X			X			
Track and follow-up longitudinal care (after primary intervention and/or treatment is complete)				X		I		X		
Uses standardised terminology to collect and codify data in a structured manner.				X						
Exposes data via openly available (authorised) APIs which can be used to retrieve/contribute data to/from other systems				X			X			
Implements standardised interfaces (HL7, FHIR, etc.) for data interchange				P	I		P			
Track the human resources of the relevant business unit within the used environment (name, employment, specialty, etc.)		X			P		I			
Integrate data between differing care settings (specialty care, acute hospital care, emergency, general practitioners, etc.)					X	I	I			
Used to report important life event trigger events of patients to MOH (births and deaths)	X				X		X			
Track the request, promise, fulfilment of drug orders (i.e., via a pharmaceutical module)						X	X	X		
Share indicator data with central public health monitoring and reporting system (example: DHIS2 or eIMMR)	X					P	I			
Store security audit data which allows for system administrators to review the access, disclosure, creation, and amendment of clinical data.							I			

	Anti-Leprosy Campaign	Health Promotion Bureau	Quarantine Unit	TB and Chest Diseases	National Dengue Control	Antimalaria Campaign	HHIMS (Architecture)	NSACP	Medical Services I & II	Planning Unit
Integrate with centralised registries for the sharing of patient, location, and provider information							I			
Requires non-repudiation of emission for data. Requires that data reported to MOH matches data user understood was being sent. Ensure that data has not been tampered after validation.										X

Annex C - List of Current Digital Health Interventions in Sri Lanka

The “Evaluation of Electronic Health Information Systems (HIS) for the Ministry of Health, Nutrition, and Indigenous Medicine – Sri Lanka (2019)” [5] provided a list of all the digital health systems interventions in use in Sri Lanka (Table 6 in that document). This information is summarised in this document below for the reference of readers.

Acronym	Name	Scope	Status (2023)	Interchange
HRMIS	Human Resources Management Information System	Institutional		None
WebIIS	Web Immunization Information System	National		None
eMHMIS	Electronic Mental Health Management Information System	National		HL7, ICD10
NHRIS	National Human Resources Management System	National		ISO3166
HFSM	Health Facility Survey Management System	National		ADX, ISO 3166
NBTSIS	National Blood Transfusion	National		ADX
CRVS	Civil Registration and Vital Statistics	National		ADX, HL7, ICD10
QHRMS	Quarantine Health Record Management and Surveillance Systems	National		ICD10
eMSRS	Electronic Monthly Statistics Reporting System	National		ADX
LeIS	Leprosy Health Information System	National		ICD10
AEIS / OPDIS	Accident and Emergency Information System / OPD Information System	Institutional		HL7, ICD10
EIMS (HIV)	Electronic Information Management System	National		ICD10
HIMS-AMC	Health Information Management System Anti Malaria Campaign	National		ADX, HL7 CDA
MSMIS	Medical Supplies Management Information System	National		None
DNMS	District Nutrition Monitoring System	Sub-National		ADX
HHIMS	Hospital Health Information Management System	National		HL7, DICOM, ICD 10
HIMS	Hospital Information Management System	Sub-National	SWASTHA	HL7, CDA, DICOM, ICD10
eIMMR	Electronic Indoor Morbidity and Mortality Register	National		ICD10
eRHMIS	Electronic Reproductive Health Management Information System	National		HL7
Cloud HIMS	Cloud Based Hospital Information Management System	In Development		HL7

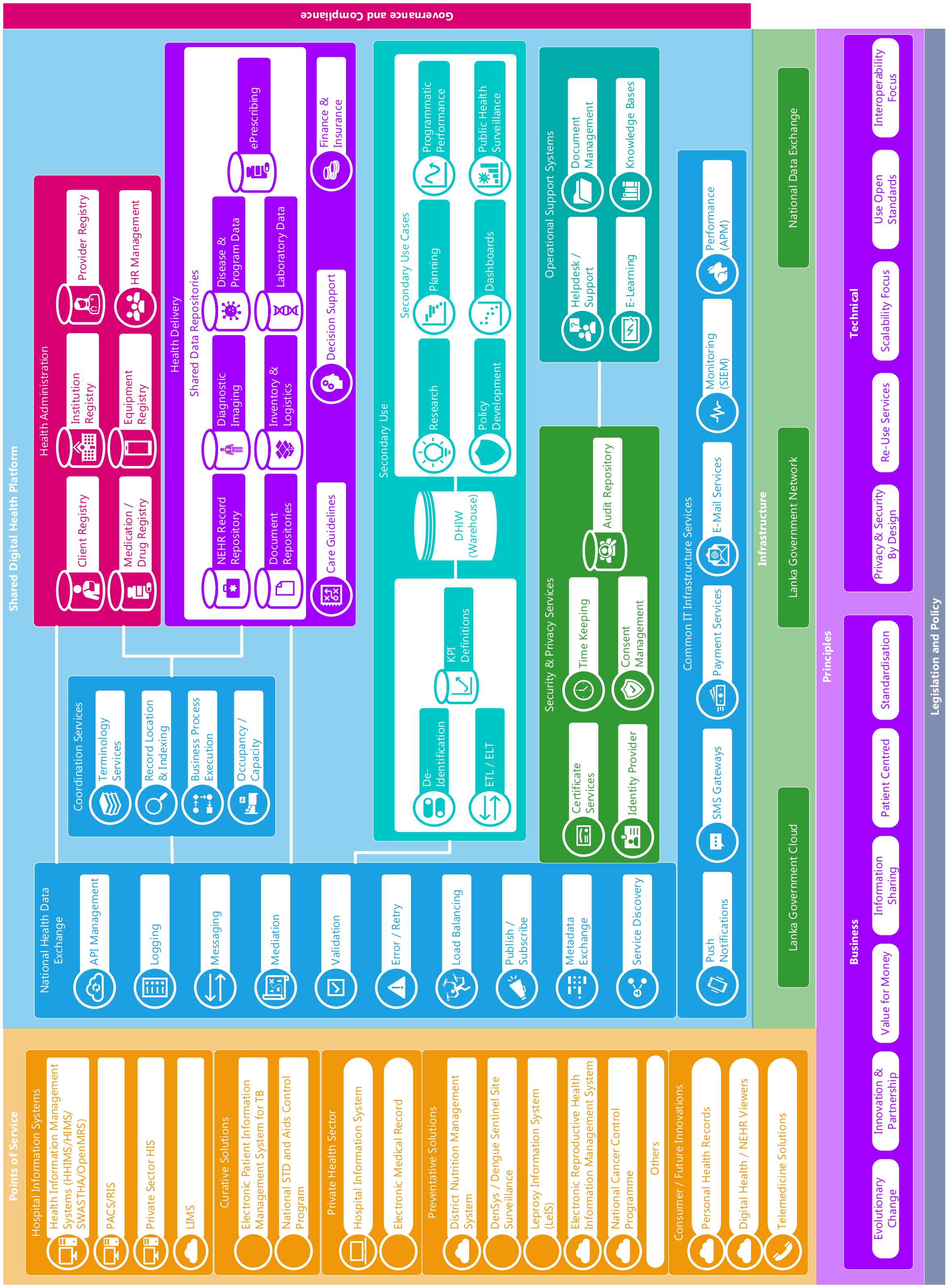
Annex D. - Blueprint Service Detailed Dependencies

Service	Depends On	Optional	Description / Rationale
Helpdesk / PM Services	Enterprise Knowledge Base	Y	Linking helpdesk services with an enterprise knowledgebase can improve IT efficiency by collecting resolutions to issues or pointing to common resources.
	Identity Provider	Y	Providing a single sign on for helpdesk and project management services reducing the administrative overhead of managing user credentials.
E-Learning Services	Enterprise Knowledge Base	Y	Linking training content to relevant content in an enterprise knowledgebase is useful for providing context and operational support for training materials.
	Identity Provider	Y	Providing a single-sign-on for the learning management system or e-learning platform reduces administrative overhead for user credentials.
	Enterprise Document Management	Y	The enterprise document management service provides document tracking, versioning, approval, and publishing services which can be linked within the e-learning content.
Document Management	Enterprise Knowledgebase	Y	The document management system may benefit from an enterprise knowledgebase solution for providing links within documents as well as publishing documents.
	Identity Provider	Y	Providing single-sign-on for the document management system reduces administrative overhead for user credentials.
Terminology Services	Identity Provider	Y	Providing single-sign-on for terminology definition, workflow, as well as the terminology APIs.
Identity Provider	HR Management	Y	Using the HRMIS (or various HR solutions) as a basis for the creation of new access credentials (on hiring) and revocation of access credentials (on termination) is a best practice.
	SMS Gateways	Y	Sending one-time-passwords (OTP), password reset instructions, and telephone verification codes from the identity provider reduces the need for independent solutions to implement the same logic repeatedly.
	E-Mail Services	Y	Sending one-time-passwords (OTP), password reset instructions, e-mail verification codes, notifications of inactivity or login, etc.
	Audit Repository	N	Provides a location for security audits (login/logout, session start/session extend/session termination) for the identity provider.
	Certificate Services	N	Required for the issuance of encryption certificates, dissemination of public keys, and digital signing of bearer/ session tokens using the RSA256 signature algorithms.
E-Mail Services	Identity Provider	Y	If providing governmental e-mail services to users, the use of an identity provider to establish access to mailboxes, IMAP or POP services is useful (i.e., provides common authentication services).

Audit Repository	Time Keeping	N	Consistent time for all events within the system is vital to understanding the order of operations between solutions in the system as well as the time when intrusions, or events occur in relation to one another.
NHDX	Certificate Services	N	Certificate services are required for the NHDX to establish a chain of trust if using node authentication (client certificates), as well as validating digital signatures (see 6.2.1)
	Identity Provider	N	Identity provider is a common dependency for all DHP services operating within the context of the NHDX. The identity provider may need to be contacted by services within the DHP for validation of session tokens, or application authentication within the NHDX.
	Time Keeping	N	Time keeping services are important within the NHDX to ensure that all services are using consistent time for all events.
	Terminology Services	N	Terminology services are common dependency for all services in the NHDX. The terminology services may be used by mediation services for validation, or by repository or registry services for mapping/validation.
Digital Health Information Warehouse / Health Management Information System	ETL	Y	ETL services may be leveraged to populate the DHIW from solutions which require active pulling of data from APIs or Databases and populating the DHIW.
	KPI Definition Repository	Y	An indicator definition repository is useful for disseminating consistent definitions, surveys, and calculations to all services within the DHP for the computation of indicators.
	NHDX	Y	All common registries within the digital health platform will require the use of common NHDX services (auditing, identity, certificates, orchestration, etc.).
Master Patient Index		N	
Facility Registry		N	
Provider Registry		N	
Medication / Drug Registry		N	
Equipment Registry		N	
NEHR Repository	Master Patient Index	N	Provides consistent identification for patients whose records are collected in the NEHR. The master patient index is used to cross-reference all citizen and non-citizen records which need to be stored in the NEHR.
	Facility Registry	N	Consistent identification for facilities providing health services in the DHP and the use of these enterprise identifiers in the NEHR is encouraged.

NEHR Repository	Provider Registry	N	Consistent identification of provider organisations and health workers which are referenced within the patient's national record.
	Medication / Drug Registry	Y	Consistent identification of medications or drugs which the patient is actively prescribed, dispensed, etc.
	Consent Management	Y	Using the consent services of the DHP will allow the NEHR to appropriately enforce policy decisions, and/or allow for the validation of tagged policies for records.
	Record Locator / Index	Y	The record locator is optional for the NEHR. Record locator and indexing services are primarily required once more than one repository of information is available for storing patient data.
Disease / Domain Repositories		N	A record locator is required when more than one repository of information for a single patient is contributing to the patients "shared" health record. Imaging and document repositories (if using IHE XDS-I) will also require this functionality.
Imaging Repositories		N	
Document Repositories		N	
Inventory / Logistics Data	Medication / Drug Registry	N	Consistent identification of approved drug products, equipment and devices is important for logistical inventory reports as well as order flows between organisations.
	Equipment Registry	N	
Consent Management	Master Patient Index	N	The consent management services will require the association of consent policies between health data, patient identity, and security principals.
	Identity Provider	N	
	Record Locator	Y	
Clinical Decision Support	Clinical Guidelines Repository	Y	The separation of a clinical guideline and the execution of the clinical guideline is described in section 4.2.5.6. It is a recommended pattern and therefore this dependency is marked as optional.
	NEHR Repository	N	CDSS (as with any rules engine) requires a series of facts (data elements in a patient profile) to execute and emit proposed actions. It is therefore required, that a CDSS system have access to health data repositories.
	Disease / Domain Repositories	Y	
Secondary Use	DHIW / HMIS	N	Secondary use services (like dashboards, surveillance rules, etc.) should depend on aggregate data stored within the DHIW / HMIS.

Annex E. - Digital Health Blueprint Diagram



Annex F . - Table of Figures