Sri Lanka Digital Health Blueprint

Version 1.0a

Enabling a healthier nation that contributes to its economic, social, mental, and spiritual development.

2022-07-29

rev. 3613

I. Foreword

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.

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 on 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, ICTA, 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 and needs 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 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)

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 ITA. 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. The blueprint seeks to be software/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 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 an informative structure within which software 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, NeHGS, HHIMS 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 citizens.

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

II. Document Information

II.1 Revision History

Primary Authors	Date	Changes	Version

eSHIFT	2022-05-18	• Initial Version	0.0
eSHIFT	2022-06-10	• Updated verbiage on architectural views section to make each view clearer and more concise. • Integrated alignment with SL-GEA document and added name for this blueprint (SL-DHB) • Updated verbiage and alignment in objectives section with the national digital health strategy 11 principles. • Added the benefits section of the blueprint. • Added (to principles document/section) the alignment with the GEA principles. • Created requirements grouping analysis document.	0.1
eSHIFT	2022-06-17	• Added guiding principles to the document • Added key definitions and concepts to context section • Added business drivers section headings and discussion of complexity of care • Added proposed solution section managing complexity • Reorganised TOC to be more readable • Added technical / functional principles from principles document.	0.2
eSHIFT	2022-06-25	• Added description of business domains • Added explanation of the assets of the blueprint and the concepts how they relate to one another	0.3

		• Started business domain descriptions in section 2. • Technical functioning principles for guiding implementation of solutions/services within the DHP.	
eSHIFT	2022-07-04	• Finalised technical functioning principles • Finalised business drivers sections • Integrated feedback from Google Docs (0.2 edits) • Documented business domains in proposed solution section.	0.4
eSHIFT	2022-07-06	• Addition of business structure current state • Further specification of the business domains and base requirements.	0.41
eSHIFT	2022-07-11	• Added proposed solution section to document section 2. • Added description of federation • Integrated changes from redline into mainline document.	0.5
eSHIFT	2022-07-15	• Added current state to data architecture • Added descriptions in conceptual architecture • Updated descriptions in the introduction/preface section • Cleaned up verbiage throughout Sections 2 and 5. • Added defining solutions views.	0.7
eSHIFT	2022-07-17	• Additional information architecture documentation added in section 4 for logistics.	0.8

		• Further specification of the security conceptual architecture, common services, health delivery domains. • Addition of table of figures in Appendix C	
eSHIFT	2022-07-18	• Finished section 3 conceptual architecture (ready for review) • Finished section 4 information architecture (ready for review)	0.9
eSHIFT with contributions from MOH Sri Lanka, ICTA, and stakeholder groups.	2022-07-29	• Review of version 1.0 for release and broader key stakeholder engagement.	1.0
eSHIFT with contributions from MOH Sri Lanka, HIU, ICTA, NTA	2022-09-03	• Integration of initial series of feedback/comments from stakeholders. • Updates to diagrams for clarity. • Inclusion for service metadata exchange/service discovery component in the blueprint. • Moved minutiae from section 4.3 to the interoperability plan (as the definition of interoperability profiles for Sri Lanka fits into that document and distracts from this document's content)	1.0a

II.2 Related Documents

#	Document Title / Link	Relevance
1	DHEAP Zero Draft 0.6	Provides the basis for this document and preliminary analysis of Sri Lankan digital health landscape
2	National Digital Health Guidelines and Standards (NDHGS) V 2. - 2020/2021	Gives a holistic view of the existing digital health policies, standards, and minimum datasets in Sri Lanka and guidelines to be followed by digital health implementors.

3	Sri Lanka Government Enterprise Architecture (V1.0, Published 25/04/2022)	Exemplary Enterprise Architecture for broader Sri Lankan Government initiatives
4	Sri Lanka National Health Policy 2016-2025	Vision and Mission of the healthcare system of Sri Lanka
5	Evaluation of Electronic Health Information Systems (HIS) for the Ministry of Health, Nutrition, and Indigenous Medicine – Sri Lanka (2019)	Referenced as a driver of current business requirements of existing systems in Sri Lanka

II.3 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 the business goal/operation rather than wire-level implementation (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).
Jurisdiction	Refers to the national, provincial, or district geopolitical area which is implementing the blueprint.
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.
Service Provider	Used to describe a service (such as a software, organisation, cloud service, etc.) which provides or exposes business functions to a service consumer.
Service Consumer	Used to describe a service (such as software, organisation, cloud service, etc.) which consumes the business functions exposed by a corresponding service provider.
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.
Serialisation	A process whereby data structure is transformed from memory into a computable form (like JSON or XML), which can be transported or saved then loaded/interpreted by another system to recreate the same structure in memory later.
ESB	Enterprise Service Bus – A pattern of SOA integration whereby service consumers and providers communicate with one another via an intermediary (the bus) which is responsible for transformation, reliable delivery, replay, and publish and subscribe services.

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 using JPEG
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 Institute	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
Data Custodian	Organisations which operate the digital health platform, or any point of service system which communicates with or stores PHI
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.

II.4 Document Licence & Copyright Notices

TODO: Insert governmental, WHO, or GF copyright notices as appropriate.

II.5 Submitting Changes / Issues

The blueprint document is publicly accessible to all stakeholders for review. Throughout the review process, and after publication of the final version, changes will need to be made to this document. It is recommended that readers propose changes via the Change Request form (Annex E) and submit these change requests to the indicated e-mail address (where you obtained this file). Change requests will be reviewed on a regular basis and entered in II.5.1 as an outstanding issue until they can be resolved.

II.5.1 Outstanding Issue List

This issue list is included for the convenience of the reader and provides insight into outstanding issues with this document for context.

#	Date	Reporter	Section	Discussion / Issues	Resolved

1	2022-07-29	Dr Palitha Karunapema	7.2	Figure 61 in section 7.2 needs to be changed to provide more output-based objectives.	
3	2022-08-05	Justin Fyfe (recommendation Pradeep Sylva)	3.1.2	Additional description of the provincial health systems needs to be integrated into the document including the types of services offered (curative, preventative, etc.). Additional documentation and description of the public health services should also be included in the baseline state. The additional description health services including: 1. Registered/non-registered Pvt healthcare including GPs practices 2. Healthcare provided by armed forces and police 3. Semi-government healthcare institutions 4. Clinics conducted by Municipalities, Universities, Prison hospitals 5. Ayurveda hospitals --> may be out of scope-->discuss	
4	2022-08-05	Justin Fyfe (recommendation Pradeep Sylva)	3.2.2	Add target functionalities / drivers diagram in a similar format to the baseline state to allow for easier comparison while reading. This diagram should be in a similar format to the baseline (taken from DHEAP) and illustrate the target functionality / drivers.	2022-09-02 – Added as Figure 8
5	2022-08-05	Justin Fyfe (recommendation Pradeep Sylva)	3.2.2.2 – (Figure 9- Sharing of Clinically Relevant Data)	Figure is too generic, should include examples from the NDGS – diagram should illustrate facility level data (detailed) being extracted and summarised for NEHR.	
6	2022-08-05	Justin Fyfe (recommendation Pradeep Sylva)	3.2.2.1.4	Discussion of opt-in and opt-out caveats and stance within the blueprint. Options include: * full opt-out (no data shared)	2022-09-02 – Added as reqs in 3.2.2.1 and 3.2.5.3

				* Specific use case opt-out (don't use data for research, etc.)	
7	2022-08-06	Justin Fyfe	All	Currently the verbiage used within the document is: domains have multiple services. I think this should be refactored so that: domains have multiple components which expose multiple services. For example, the Health Administration Domain with the Master Patient Index Service should be refactored to the Health Administration Domain with the Master Patient Index Component which exposes patient administration services.	
8	2022-08-06	Justin Fyfe (recommendation from Palitha)	5.1	Figure 37- Baseline Information Architecture needs to be updated to: ● Add additional information systems (OpenMRS, disease systems, etc.) ● Use separate symbology for applications and other data objectives/programs (like surveys) ● Indicate those systems which are relevant to the DHP however not in scope for specification of the DHP (such as other ministries)	
9	2022-08-06	Justin Fyfe (recommendation from Chaminda)	5.2	Add a diagram to the information architecture which is similar in format to Figure 37- Baseline Information Architecture showing the future state so readers may easily see the transition from the current state to the future state.	

10	2022-08-06	Justin Fyfe (recommendation from Chaminda)	5.2.1	Add a section to the information architecture which clearly defines the role of information policy. This section should contain: ● How information policies are applied to data to fulfil the requirements of the data protection act ● Examples of policies for sensitive data (such as VIPs, taboo diagnosis, etc.)	2022-09-02 – Added link to policy tags value set. Updated description to point to technical details.
11	2022-08-06	Justin Fyfe	5.2.1	There should be more discussion regarding the storage of provider organisations and how they relate (or don't relate) to health workers (who are also providers). Potential that the provider registry be further de-composed into Worker and Organisation registries with an interlinked registry component to facilitate health service discovery for e-referrals.	
12	2022-08-07	Justin Fyfe	4.3	Re-organize content concerning evolution of blueprint and development of platform services, move appropriate content into interoperability plan and domain development guides where required	2022-09-02 – Resolved, sub-sections of 4.3 have been moved
13	2022-09-01	Justin Fyfe (recommendation from Udara)	3.1.1	Scope of ICTA in the project should be described in the business structure documentation so the reader understands the scope of the agency within context of the blueprint.	
14	2022-09-01	Justin Fyfe (recommendation from Pradeep Sylva)	3.1.1	Also mention about (here or in sections above) 1. Pvt healthcare providers liaised through a specific Director of MOH and other non-registered GPs	

				2. Other relevant ministries and state corporations 3. NGOs, funding agencies and donors 4. Solution providers, suppliers, universities, innovators 5. Patient groups and public	
15	2022-09-01	Justin Fyfe	3.3.4	There is an open discussion regarding the most appropriate manner in which the DHP can be geographically scaled across Sri Lanka. Federation provides an opportunity for localised instantiations of the DHP for sub-national purposes. However, we want to ensure that we find a good balance between complexity (having too many layers of federation) with desired functionality.	
16	2022-09-01	Justin Fyfe (recommendation from Pradeep Sylva)	3.3.5	Adding a new architectural domain for inter-governmental integration services to specify linkages to other domains (Justice systems, CRVS, etc.) should be considered and discussed somewhere. Either as a new architectural domain, or within an existing domain (such as data exchange)	
17	2022-09-01	Justin Fyfe (recommendation from Pradeep Sylva)	3.3.5.2	Recommendation was to add Ethics to the domain title. Unsure if this is the correct verbiage since these services would support the ethical use of data via enforcement of privacy and security policies.	
18	2022-09-02	Duane Bender (recommendation from Dr Palitha	7.4.2	As a supplement, provide a procurement checklist or similar tool that will be required to be filled out before giving approval for new software purchases to ensure alignment with proposed overall architecture. Considerations should include interoperability profiles, total cost of ownership, privacy and	

				security, accessibility, platform, data stewardship and governance, etc.	
19	2022-09-02	Justin Fyfe	4.2.4.1	To be discussed: The role of biometric data in the identity and resolution (or authentication) of subjects of care. This is a commonly discussed topic for MPI, and it would be useful to continue the discussion in how the biometric data from UDI can be stored and linked with MPI (perhaps it belongs in the MPI solution view and just called out in this document?)	
20	2022-09-04	Justin Fyfe (recommendation from Chaminda)	5.2.4	Need to verify alignment with the current ordering management to see if the proposed future state is compatible with the work for logistics management and supplies.	
21	2022-09-13	Dr. Hasitha Promod	4.2.2	It would be good to include explicit examples of the architectures for the hospital information systems, OpenMRS and PACS in use within facilities / clusters and how they align and operate within the blueprint environment. Currently there is some verbiage about RIS and points of service – however calling out directly the OpenMRS architecture would be helpful for readers to gauge alignment.	
22	2022-09-13	Dr. Palitha	New	It would be helpful to add a section which allows readers to self-assess their own alignment to the blueprint. A checklist would be greatly helpful in assisting in this type of exercise. Also in the realization section it would be helpful to include documentation regarding the the governance and	

				operationalization (new organization or extension of existing organization).	

Table of Contents

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 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 is provided by the public sector[2], which handled more than 6 million hospitalisations and over 55 million outpatient visits in 2017[3].

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.
- *Capacity Building* – Undergraduate supportive hospital base training and full time In-service training of health professionals.
- *Supportive Services*: 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 353 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.

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

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 a Minister of Health and a Secretary of Health, the latter being a senior administrator from the Sri Lankan administrative service or a doctor who also is a specialist administrator.

The Director General of Health Services (DGHS) is the technical head of the Ministry and is supported by multiple Deputy Directors General (DDGs) who are 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 are nine provincial ministries of health which are under the leadership of a provincial Ministers of Health. Provincial health councils are permitted to formulate their own statutes which function within the boundaries of national health policy.

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 patients.

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. Digital health related activity is the main responsibility of the medical informatics specialty in parallel to the global trends and played a main role in the development of this blueprint in collaboration with some international technical assistance (ITA).

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.

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

The vision is to establish a health information system (HIS) which augments an effective, equitable, economical, and quality service while ensuring privacy and confidentiality of care recipients. The national policy set forth objectives including:

- Ensure that 50% of 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 50% of base hospitals, district general hospitals, provincial general hospitals, and teaching hospitals.
- 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 key strategic areas and was summarised in the Digital Health Enterprise Architecture Plan [1] and are shown Figure 1Figure 1, identifies the following goals:

- Strengthen service delivery to achieve preventative health goals
- Appropriate and accessible high quality curative care for all Sri Lankan citizens
- Promotion of equitable access to quality rehabilitative care
- Ensure a comprehensive health system through a better restructuring of HRM
- Develop strategic partnerships with all providers of care

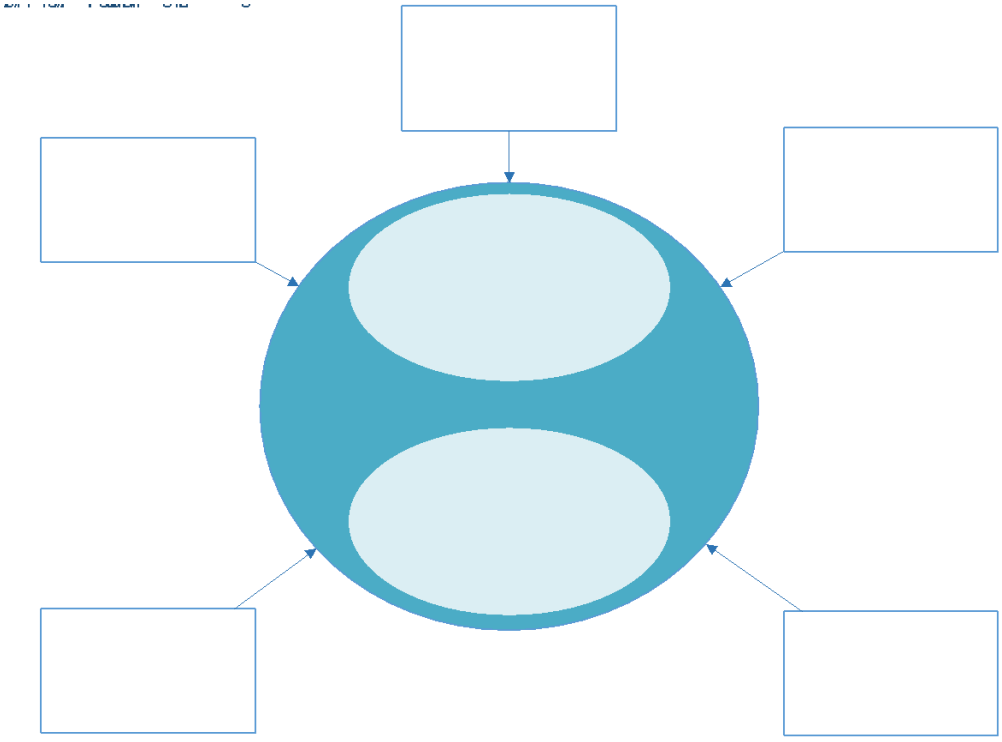

Figure 1 – Main Strategic Areas of National Health Policy[6]

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.

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 (0), 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 (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.

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

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 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.

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 (Pronto) 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. Additionally, without a wholistic integration between care delivery services and stock management, it is difficult to create forward looking stock forecasts for clinics and facilities.

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 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:

- **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.
- **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.
- **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:

- **Inform** clinical providers and administrators decision-making process via access to the digitised, connected, and shared data.

[8] PG 3569 Health Policy (E) new.indd (documents.gov.lk)

- **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.
- **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. Solution 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 2provides 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.

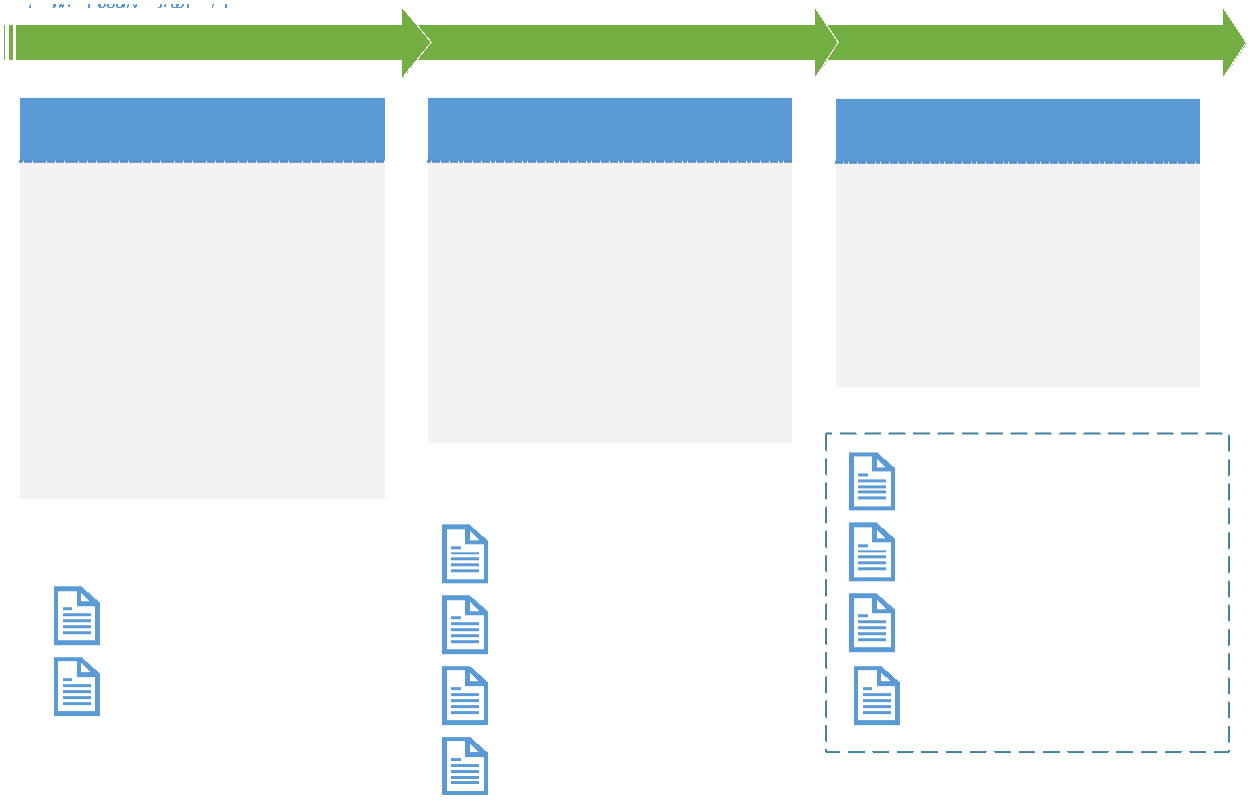

Figure 2 – Architectural Levels and Artefacts

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
Solution 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 building blocks, frameworks, patterns, principles, and concepts upon which digital health services in Sri Lanka will be integrated. The enterprise view encompasses:

- *Architecture Vision & Context* – These serve as the basis for alignment of the entirety of the digital health ecosystem in Sri Lanka. This allows decision makers and planners to assess the alignment of a particular solution with the overall vision of the enterprise.
- *Objectives & Business Drivers* – Enterprise requirements are used to describe the requirements of the national digital health architecture and how they relate to the business requirements of Sri Lankan stakeholders.
- *Enterprise Services* – Defines the overall building blocks of national, provincial and organisation components and how they fit together.

- *Business Domains & Organisation* – Defines the sub-categorisations or areas of concern for the enterprise blueprint. Domains are used to describe the business domains of the digital health ecosystem which facilitate the realisation of the enterprise requirements.
- *Conceptual Enterprise Information Architecture* – Identifies a common set of entities, and their related principles in terms of management and use within the Sri Lankan health ecosystem.
- *Enterprise Functional & Technical Principles* – Articulates the vision and strategy for operationalisation of the blueprint including roadmaps, cross enterprise use, and manifestation of the blueprint through logical and physical levels.

The enterprise view is comprised of two key documents used to disseminate the vision to relevant stakeholders – the Digital Health Blueprint and the National Interoperability Plan. A description of the contents of these documents is provided in Table 2.

Table 2 – Enterprise Architecture Artefacts

Document	In Scope	Out of Scope
Digital Health Blueprint	• Architectural Vision • Strategic, Business and Functional Principles • Enterprise Business Requirements • Domain Definitions and Descriptions • Operational Vision • Realisation, moving from current state to envisioned future states	• Detailed solutions architecture • Detailed use cases, business process flows. • Detailed system to system data flows. • Prescriptive standards selection and specification.
National Interoperability Plan	• Analysis and guidelines for the selection and use of appropriate standards. • Applicability of standards for each health domain • Guidelines on the standards development process • Patterns for data exchange between blueprint building blocks (documents, messaging, imaging, transport, etc.)	• Profiling of standards • System to system data flows, trigger events, and data elements. • Code lists, minimum data sets. • Test cases, certification requirements.

	• Security considerations specific to each standard domain • Validation, testing and certification processes and planning	

2.3.2 Solution Views

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

The primary goal of the solution view is to attain *business interoperability* between all involved systems for a particular enterprise service. 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 solution 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.

Another goal of the solutions views is to provide further detail for a particular business function within the overall enterprise architecture in a manner which is implementation agnostic. This decouples and insulates the business objectives of the solution from implementation considerations (for example programming language, toolkits, or detailed standard profiling).

Once a collective understanding of the clinical and business domain is attained, one or more implementation methods (HL7v2, HL7v3, CDA, HL7 FHIR, DICOM, web services, etc.) can be developed using the most appropriate mechanism for the selected implementation (for example, if FHIR is selected then a FHIR IG should be used, if DICOM is selected, a DICOM profile should be leveraged or documented). Solution views also provide scenario-based examples in non-technical, clinical/business friendly language of the intended use of the services in the digital health platform.

Solution View documents should contain:

- *Solution Business Architecture* – Applications of the specific solution are described as a series of use cases using the actors defined in the enterprise architecture. These application descriptions serve as the basis for understanding the business processes for the domain, and the requirements of the solution. Assets in the business architecture include:
    - Actor definitions (including their objectives, skills, and intent)
    - Use cases defining the specific use of the EA within the business domain
    - An overall picture of the business domain (how actors relate to one another)
- *Solution Services Architecture* – Identifying the specific integration patterns (messaging, documents, etc.), technical actors (systems and users), triggers (processes and events), and behaviours of the solution domain. Assets in the solution services architecture include:
    - Clinical storyboards identifying exemplary scenarios where the services are used

    - Service actors (system types) which participate in sharing data
    - Business objectives of the APIs exposed and used by the services
    - Orchestration / Sequence of message flows
- *Domain Information Architecture* – Specifying the detailed logical entities, their data elements and requirements, and relationship to other entities. Assets include:
    - Trigger definitions of message flows in the enterprise.
    - Data requirements for the solution (data sets, vocabulary, etc.)
- *Operational Considerations* – Specifies the network patterns, queueing, matching, configuration, security, and privacy considerations which would be required to operationalise the solution. Assets in this section typically include:
    - Security considerations (auditing considerations, access controls, etc.)
    - Cross-system considerations (notifications, e-mails, SMS, etc.)
    - Privacy implications and protections

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 service. The technical view should contain:

- *Physical Design* – Which describes the networking topology, server or cloud infrastructure used, ports, domain names, etc. When using the Lanka Government Cloud (LGC) and Lanka Government Network assets, the physical architecture should document the services used and the way shared government services are leveraged.
- *Privacy / Security Implementation* – Describes the concrete implementation of the security environment at a physical layer (networks, gateways, firewalls, etc.) as well as software (role-based access controls, policies, etc.) and messaging (auditing, authentication methods).
- *Software Design* – Which describes the implementation of the software services. If using common off the shelf software, this should represent or reflect the configurations and/or customizations of the software being deployed.
- *Standards Profiles and APIs* – Documents the concrete patterns of integration including the standards selected, the profiling of such standards, the transport and security considerations of the data exchange, etc. Assets include:

The technical view may be expressed in a format appropriate for the implementation/realisation of the domain. This can include:

- Specific implementations of the architecture (URLs, security requirements, access controls, certification requirements),
- Standards specific specifications (FHIR IG, IHE Volume 4 content, etc.)
- Code lists and standardised terminology
- Software Requirement Specifications or Functional Design Specifications for software interfaces

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.

[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 Comments | Ministry of Health and Family Welfare | GOI (mohfw.gov.in)
[14] Profiles - IHE International
[15] Digital health platform handbook: building a digital information infrastructure (infostructure) for health (who.int)

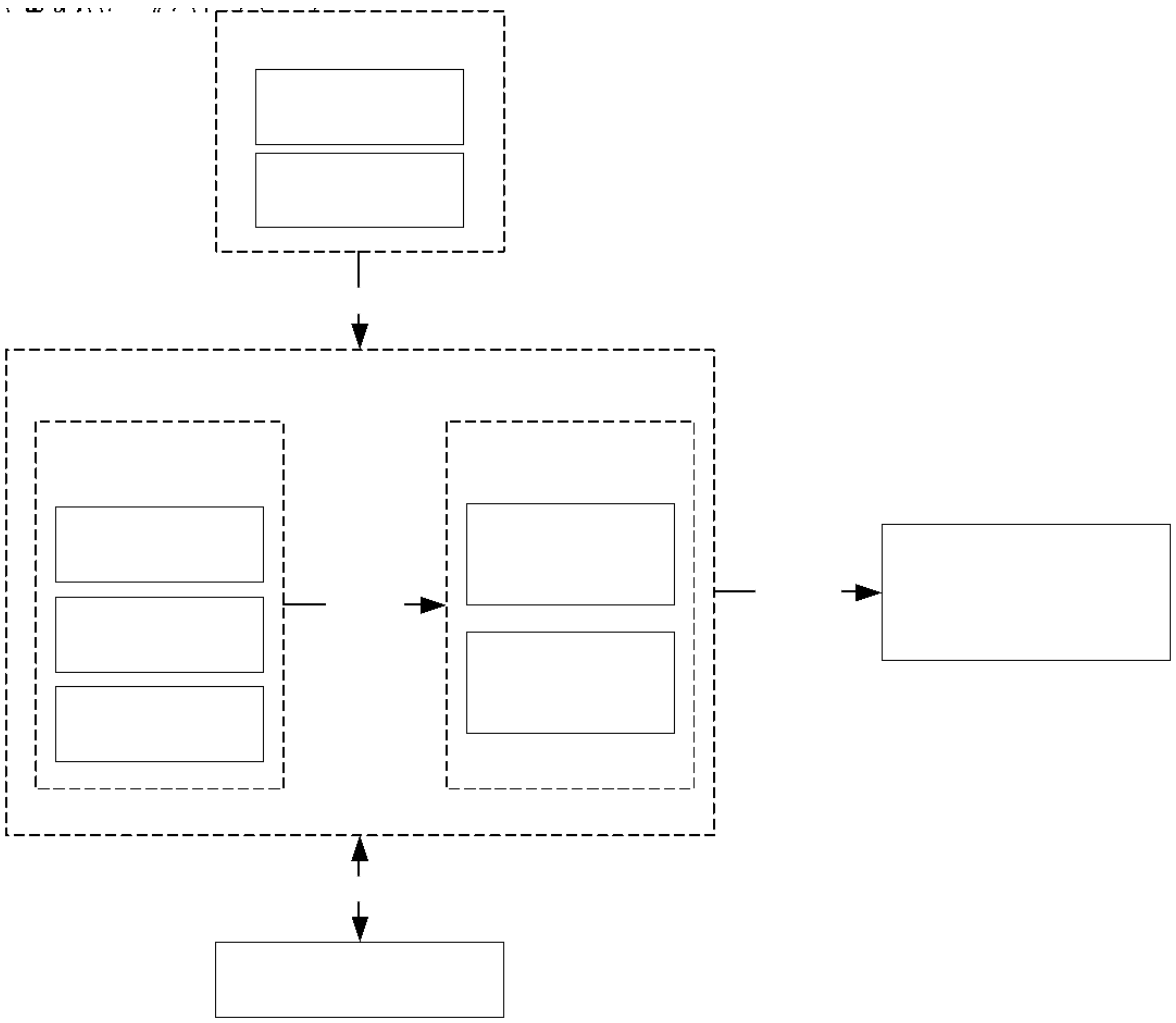

Figure 3 – Relationship of Blueprint Concepts

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 29).

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 grows 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 55).

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 ICTA resources (Lanka Government Cloud, Lanka Government Network, National Data Exchange Services, etc.) 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 ministerial agencies or the private sector.

Examples include:

- HHIMS – Hospital Health Information Management System
- HIMS – Hospital Information Management System
- Cloud HIMS
- ERHMIS for reproductive public health
- LeMIS – Leprosy Management Information System
- EIMS – HIV Electronic Information Management System
- WebIIS – Web Based Immunization Information System
- ePIMS – Electronic Patient Information Management System

An assessment of digital health interventions found in Sri Lanka can be found in the HIS Evaluation 2019 (referenced document #4) and is summarised in 0 of this document.

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 may vary depending on the use case of data in a particular context. The term DHIW is used to encapsulate all secondary use and reporting mechanisms within the DHP. Technologies which may 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. Interested parties 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 Baby Chandra 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 may 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 may be monolithic in nature (where only one repository exists for all clinical information), may be federated (between provinces, districts, or jurisdictions), may be delineated across disease specific vectors (such as Non-Communicable Diseases, HIV/AIDS, diabetes, or immunisation) or may be a specialised point of service where a test/procedure was performed (such as a PACS or RIS in a hospital system, a digital pathology lab, etc.).

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 in near real-time 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 may apply to the various individuals, organisations and stakeholders that may 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 primary 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 how a national digital health system may be realised and enables stakeholders and project teams to begin to envision how their systems may 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

It is envisioned that 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 if desired.

2.6.1.5 Framework for Education, Training & Skills Development

The Blueprint can help to provide a framework for education & training and capacity building in digital health. Common terminology and concepts can be introduced into various skills development programs across the country which will aid in the transition to a digital health environment.

2.6.1.6 Vehicle for Participation in the International Community

With the development of a blueprint and interoperability plan, Sri Lanka will be well positioned to engage with the international health informatics community. Engaging internationally will enable Sri Lanka to stay ahead of changing standards and technology. The international community disseminates knowledge and experiences learned in other jurisdictions and distributes industry specific tools and best practices.

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 and their advocates and supporting organisations (for example, Sri Lanka Federation of the Visually Handicapped) to be aware of the future

digital health infostructure and to help envision use-cases that will provide the best care for all. This may include innovative applications that make use of the data contained in the infostructure, allowing a future opportunity for patients to view their own clinical records in specialised tools customised to their condition, as well as providing future opportunities to provide digital proof of procedures, prophylaxis, immunisation records etc., aligned with the desires of the citizens and government policies. Patient support groups may also envision future uses of the infostructure that integrate and deliver expertly curated content custom tailored to specific patients and their conditions.

2.6.2.2 Benefits for Central 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 jurisdictions in Sri Lanka. The architecture assists in manifesting the national digital health vision and mission into a tangible framework for architecting and deploying digital health services. Use of a common blueprint enhances and accelerates the development of digital health services and applications within the national digital health strategy, providing a comprehensive national strategy and guidance that can also be leveraged throughout provincial and regional initiatives.

The Blueprint can be used as a tool to assist in achieving stakeholder consensus on national strategies and priorities and help to establish a prioritised roadmap to make the most effective use of limited resources and funding. The Blueprint will assist in guiding national digital health investments and allow for donor alignment to national investment priorities.

A common blueprint helps to identify reusable, sustainable and scalable digital health elements to expand and build upon what has already been accomplished, while also assisting in addressing and planning for the incorporation of innovative technology into the healthcare system as it becomes available.

The Blueprint facilitates alignment of all in-country digital health innovations to help achieve national digital health goals and provides a comprehensive view of national digital health services programs and operations. This assists in providing clarity to business services requirements, roles, responsibilities, and governance of health information systems 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 and subsequent roadmaps provide clarity and direction to technology innovators, software development organisations and solution vendors, thereby lowering the costs, timeline, and risks of systems development and/or procurement.

One of the ways 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 a common 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.

Driving towards commonly defined national standards for health information also drives efficiency in procurement, training, and reusability of solutions across the country.

The consistent use of terminology and nomenclature in solutions also improves understanding and communications within care teams and across organisations, and ultimately improves accuracy in national reporting.

Having a blueprint allows technology developers to better understand where their solution fits within the broader national digital health infrastructure.

2.6.2.4 Benefits for Healthcare Organisations

Healthcare organisations benefit from having a national blueprint in many ways. Groups such as 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 can assist in identifying business and technical requirements for new systems development activities or procurements occurring in healthcare organisations, and it can help to identify opportunities for integration of clinical or operational workflows and systems into regional or national infostructure.

The Blueprint can be used as a change management and knowledge transfer tool to aid in the adoption of digital processes by healthcare professionals, including physicians and nurses, by describing the broader benefits of a national infrastructure, such as reducing data errors and duplicate procedures, providing known identification of the subjects of care, ensuring consistent use of terminology and design patterns and providing access to information that is suitable to be shared across organisations.

2.6.2.5 Benefits for Clinicians and Healthcare Providers

Publishing the Blueprint provides a common framework and set of consistent terminology 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 will allow providers to use shared infrastructure and practice medicine between organisations and locations convenient to their own practice (i.e., telemedicine, or remote medicine services). Additionally, the introduction of streamlined access credentials will reduce the burden of remembering multiple logins, changing passwords, or updating contact information.

Further, a dual authentication process will prevent illegal access to the online clinical information systems by the unauthorised imposters.

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 Associations

Health associations such as professional colleges, credentialing agencies and other provider associations 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.

Health associations can also use the Blueprint to 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. Hospitals and public health institutes 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

2.8.1 Defining a Digital Health Enterprise Architecture Plan (DHEAP)

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.

2.8.1.1 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, Family Health Bureau, 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), ICTA and more.

2.8.1.2 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].

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

2.8.1.3 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

2.8.2 Creation of the Digital Health Blueprint

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.

2.8.2.1 Establishment of Architectural Principles

The work conducted during the DHEAP included establishing a set of guiding principles. The guiding principles consist of both strategic and technical principles and were derived through review of Sri Lankan Health Information Policy, consultative meetings and literature review conducted for Digital Health Guiding Principles in published work, as well as work published by other jurisdictions and digital health organisations. A thematic analysis was carried out to identify similar and important themes covered in these publications.

This foundational work led to the strategic and technical principles established in this Blueprint.

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

2.8.2.2 Development of Enterprise View

The initial development of an Enterprise View for the national digital health system of Sri Lanka started in 2018 with a desk review of the available digital health systems. Digital health information systems in the country were listed and these were categorised according to the WHO classification of Digital Health Interventions.

A detailed evaluation of the digital health systems available in Sri Lanka was also carried out in early 2019 using the MAPS toolkit[18] as the primary evaluation tool owing to its focus on Scale-Up. MAPS tool kit was logically mapped to the Principles of Digital Development for interpretation and the questionnaire was adopted with minor changes.

Based on these two studies, the building blocks for national scale-up were identified. Baseline architectures were developed based on the information gained through the work mentioned above through a series of discussions and meetings. The following architectural artefacts were created:

a) Business View- Entails a higher-level view of the processes involved in the healthcare provision the country across different sectors and stakeholders
b) Solutions View- Entails a view of the current digital health solutions in place and their interactions in healthcare provision
c) Information View – entails a high-level view of the current state of the information flow across domains

The current or “baseline” architectures were circulated for comments of the wider Informatics community. The diagrams were improved on the comments received and presented at a Bootcamp held in October 2021. Further comments were received at the bootcamp, and a consensus was reached on the baseline “current” architectures of all 3 views subjected to minor changes.

These views were then incorporated as valuable input into the development of this Blueprint.

2.8.2.3 Development of Interoperability Plan

Currently, the main document used for digital health standards in Sri Lanka is The National Digital Health Guidelines and Standards Version 2 [2]. All digital Health activities are planned according to these guidelines and standards. For example, the standards describe the format to be used for a personal health number (PHN) for a person. All health information systems are expected to be able to create, search and edit details of patients using this PHN, and the format of the PHN used in any health system should follow the standards documented in National Digital Health Guidelines and Standards. The Health Information Unit has also been experimenting with HL7 FHIR profiling to implement the interoperability standards of Health Information Systems in Sri Lanka.

The Blueprint and Interoperability Plan will build on this work to further define approaches to national interoperability. Subsequent documents developed as Solution and Technical Views will be highly prescriptive of technology standards, structures, and terminology to be used to achieve national interoperability.

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

2.8.2.4 Development of Solution Views

After the development of the enterprise view of the blueprint, the templates, and processes for the creation of the more detailed solution views will be undertaken. The team will define templates for the solution views which will be modelled based on:

- National Digital Health Guidelines and Standards [2] for Minimum Data Sets
- Existing Solution Requirements Specifications from Sri Lanka (for Provider Registry, Terminology Services, etc.)
- Canada Health Infoway Standards Collaborative documents
- HL7 FHIR Implementation Guide Contents for the International Patient Summary (IPS)

As described in section 2.3.2 (on page 32), these templates contain the logical construct for the business domain/problem being specified.

2.8.2.5 Development of Technical Views

Once the development of the solution views is complete and the storyboards, triggers, data elements, and business considerations are completed the TWGs will continue with the development of specific enterprise technical views.

It is expected that most of the standards used for primary integration with the DHP will be HL7 FHIR based, meaning that these technical views will take the form of FHIR Implementation Guides (IG).

Representatives from the MOH, ICTA, and other development groups took part in several HL7 FHIR IG development workshops during the development of the blueprint document. This training will be leveraged to adapt the solution views (with data elements specified from the National Standards and E-Health Guide [2], and integration sequence diagrams from the solution view itself) into consumable FHIR IG content.

The technical and solutions views are being developed concurrently.

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.

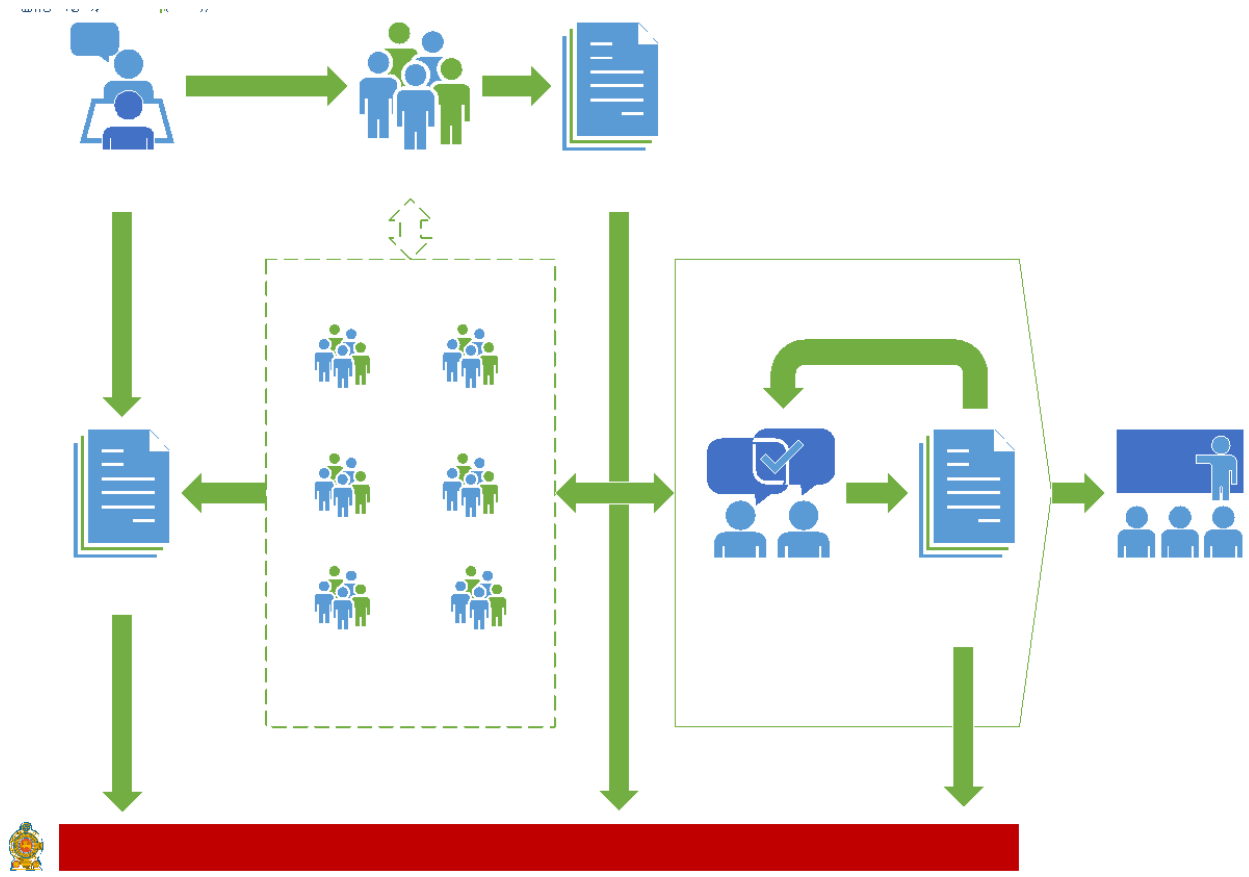

Figure 4 – Stakeholder Engagement Plan

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, Hospitals (Teaching, District and General)
- Vendors including: ICTASL (PVT) LTD, SL-CERT(PVT) LTD, TRCSL, HISSL, SLCHI
- Patient Groups
- Trade Unions
- Other Stakeholders: 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.

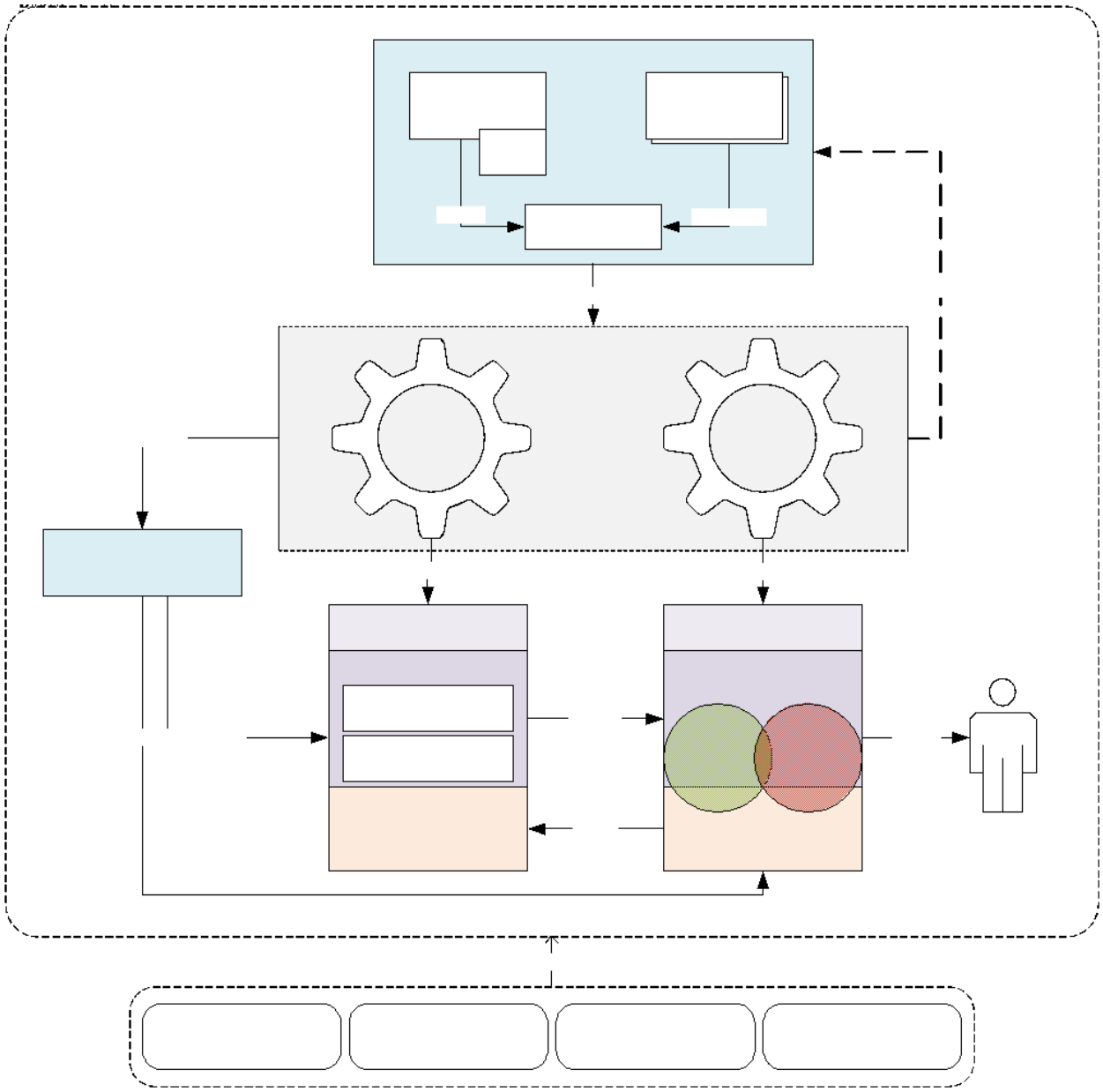

Figure 5 – Current Enterprise Business Architecture

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[19]. 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[20], which provides an in-depth view of the organisational structure of the Ministry of Health which was summarised in section 1.1 on page 21 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.

[19] PG 3569 Health Policy (E) new.indd (documents.gov.lk)
[20] *9789290228530-eng.pdf (who.int)

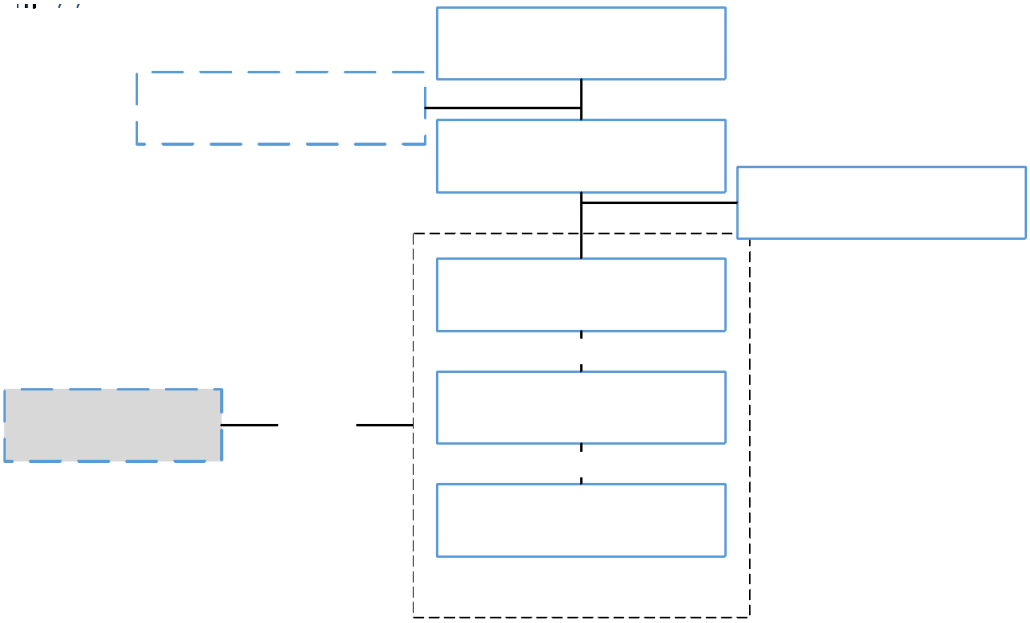

Figure 6– Conceptual Relation of Central MOH

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.

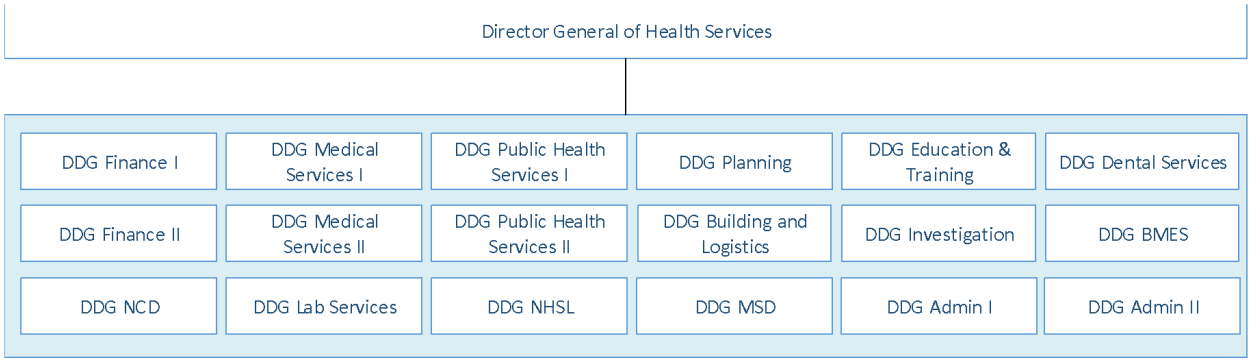

Figure 7– Focal DDGs for the blueprint

The primary areas of concern for each DDG at the central level is described in Annex A (page 182).

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 184) 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) for all Sri Lankans
- 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.

These business drivers are visualized in Figure 8, and illustrate a how these drivers relate and enhance the current business architecture.

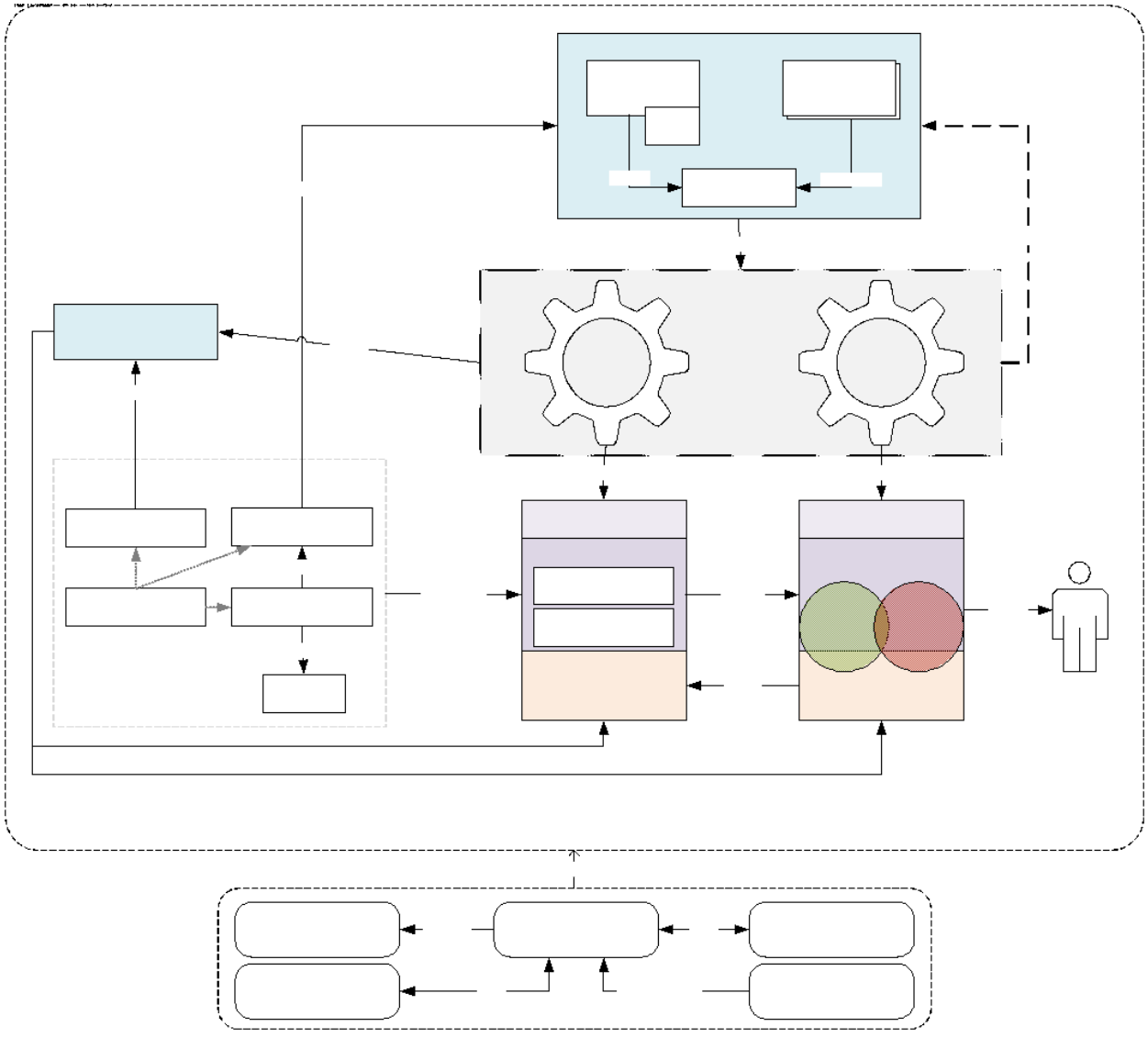

Figure 8 - Business Drivers / Future State

3.2.1 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 clinical settings (hospitals, clinics, outreach, etc.). A provincial or national solution needs to take into consideration the ability of a solution to operate in any of these settings while providing consistent and timely access to data.
- *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 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 72.

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

The goal of the DHP in Sri Lanka is the support a patient-centred ed National Electronic Health Record (pc-NEHR). This electronic health record should be cross-cutting between connected organisations, software solutions, and delivery all systems, providers, organisations, and governmental bodies. NEHR will also facilitate primary health care reorganization currently undergoing within the ministry of health. The NEHR will be accumulated from contributions driven by care events delivered from birth until death - a life-long health record.

It is common in medical practice to view individual data elements about a patient as having diminishing value over time (i.e., events and observations become less relevant as the patient ages), however with the rise of cost-efficient storage, and robust archiving methods it is now possible to provide this data secondary uses beyond the first clinical use.

The nature of the DHP means that jurisdictional monitoring programs, clinical research, disease planning and prevention programs, device and drug recalls, and planning units may use historical data to make decisions based on long histories of data. Authorised secondary use of clinical data, with the consent of the patient or mandated by law and in particular the Personal Data Protection Act -March 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 goal of establishing a lifelong patient centric NEHR for a patient requires the consolidation of a lifetime structured and unstructured data, documents, documented goals (smoking cessation, etc.) and notifications. Since this could represent an immense amount of data about an individual, it is a requirement that only data which can be used to paint a clinically relevant picture (i.e., sufficient for another provider to make a clinical decision – a minimal dataset) of the patient's current and past health status should be captured and supported by the DHP.

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

- A historical index of hospitalisations including summaries of discharges.
- Blood type, allergy, immunological and prophylaxis profiles.
- Communicable disease status and diagnosis.
- Chronic conditions and care plans related to long term care.
- Critical observations related to problems and concerns.
- Medication profiles including prescriptions, dispenses and refills.
- Laboratory, pathology and diagnostic imaging test results and orders.
- Referrals and transfers between care settings.
- 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. Only those readings which provide evidence of a diagnosis or treatment decision should be shared.
- Discrete data about business processes within an institution or care setting such as daily scheduling, staff time tracking, patient transfers within a ward, nurse round schedules, etc. Only data which may provide context to a broader audience should be shared (such as transfers to ICU, donor notifications, discharges, referrals, or data used to make a clinical decision which impacts the patient's long-term health)

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 9. The initial specification of the minimum dataset for these classifications of data to be submitted to the NEHR is specified in the National Digital Health Guidelines and Standards [2] document[21].

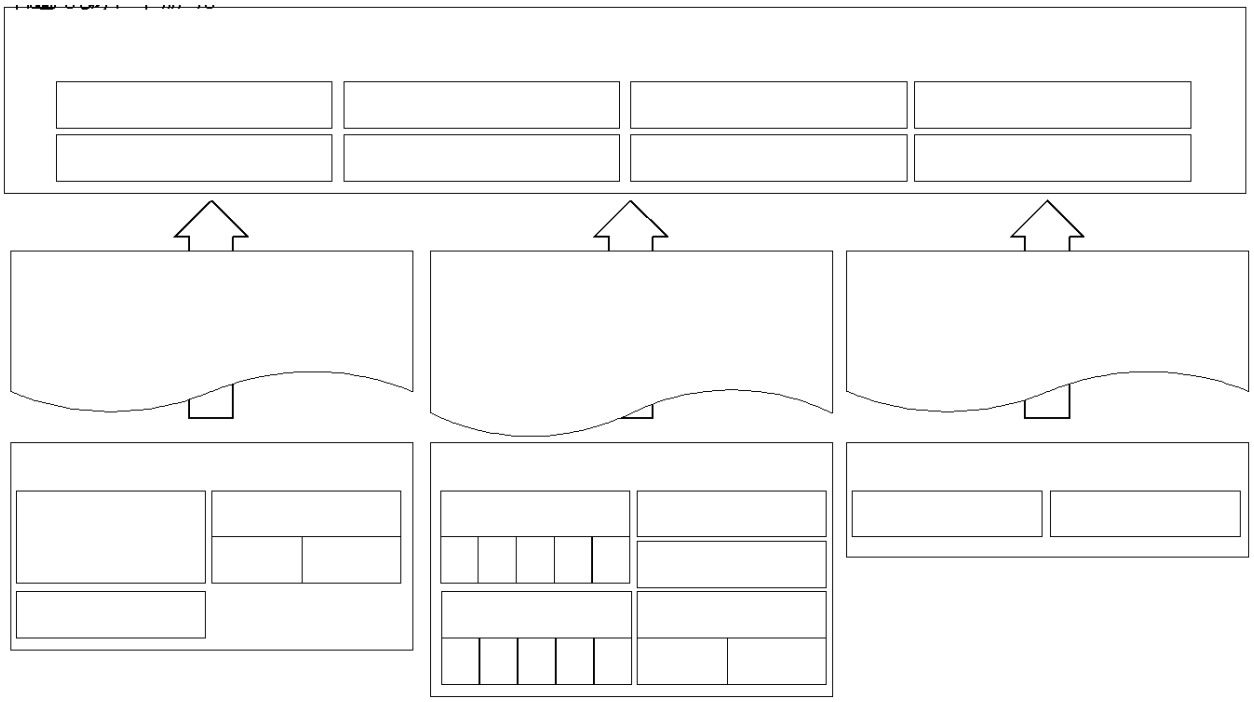

Figure 9- Sharing of Clinically Relevant Data

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 solution 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 solution 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.

[21] National Digital Health Guidelines and Standards [2] Section 7.7

- The DHP shall specify in its solution 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 may seek curative and preventative care within the public or private health systems. During treatment, patients may interact with a variety of solutions including hospital information systems (HMIS, HHIMS, 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 ensured. The DHP should support 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 may also be used to report provenance to the end user of the data in question[22].

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 may impact the decision-making process of downstream users of the information.

For example, a patient receiving treatment for cancer may have several encounters with care facilities. During these care episodes, hourly recordings of the patient's vital signs, administered drugs and procedures may occur. At the conclusion of each visit (i.e., on discharge) a summary of the events should be prepared by the discharging physician via a discharge summary.

At a later time, a primary care physician reviewing information may be interested in a summary of improvement between visits, rather than individual recordings during the visit.

In this example, the primary care physician should be made aware that the summary trend is being generated by the software rather than signed and verified by a physician. The primary care physician may be provided an opportunity to review the source of each data point in the summary which would render the source data (the discharge summaries) from which the data was obtained. The source data should be indicated as validated and unchanged since reviewed by the discharger.

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 may have been made. Once submitted, signed data should be considered unalterable, and changes should be submitted as

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

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 may be a need for the DHP to facilitate 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.

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.

For example, if a patient presents to a cancer treatment centre, is also HIV positive the DHP should return this state to the cancer centre's point of service. If the provider or cancer treatment centre lacks appropriate policies to access the HIV diagnosis, the DHP should inform the point of service that the health summary for the patient is incomplete, or that there is additional information available. The rationale for the incompleteness of the result should also be expressed in some manner (for example: Policy prevents the complete disclosure of this patient's record).

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 which may inhibit care or 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 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[23].

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) may 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 can 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. Examples include BitLocker, LUKS, or TrueCrypt.
    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

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

operating system is breached, the database contents cannot be dumped. Examples include Transparent Data Encryption (TDE) or Always Encrypted.

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. Examples include: pg_crypto, Java Cryptography Architecture (JCA).

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. Example strategies include:

a. Key escrow: Where private keys required to decrypt/encrypt data are held by a trusted third party and only provided in certain circumstances.

b. Key on client pattern: Where the private keys required to decrypt/encrypt data are never disclosed to the central DHP infrastructure, and rather, held on the client which submitted the data. This is useful in cloud environments where sensitive data should not be accessed by system administrators or operators.

- Access Control: Whereby access to certain systems, functions, or even data is blocked by 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 DHP service is not specified in the blueprint, other than specifying that the need for either RBAC or PBAC is required in DHP services and a mechanism of sharing user credentials (with policies, roles, etc.) is used. Further specifications may be elaborated in the solution and technical views for each domain.

3.2.5.2 Private

With the introduction of a, DHP it will become easier than ever before to collect, store and analyse large sets of data about individuals – i.e., "personal information." Personal Information (PI) is generally considered to be information about an individual that is recorded in any form and can include items such as name, address, employment history, biometric data, medical diagnoses, and even personal opinions. Although these data sets facilitate more efficient digital health systems and brings benefits to citizens, they also introduce potential privacy risks through misuse of that information. Many citizens feel that individual privacy is not a right that should be traded away in the name of innovation, efficiency, or commercial gain. Protecting the privacy of personal information is also a legal requirement, and in all cases, it is essential to ensuring public trust in important institutions. Privacy differs from security in that, while security is intended to protect IT assets (execution, transmission, etc.) privacy is intended to protect the disclosure of, or access to, personal information by unauthorised parties. The Personal Data Protection Act – March, 2022[24] sets the legal framework within which the privacy of health clients and providers are protected and is described in the following section.

[24] PL 012913 Personal Data (Act) Cov.pmd (documents.gov.lk)

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, but also applies to controllers or processors that are domiciled in, incorporated in, or offer goods or services to, persons in Sri Lanka. The Act applies to businesses and does not apply to personal information processed "purely for personal, domestic or household purposes" by an individual. PDPA Act applies to all commercial activity regardless of the size of the organization.

The PDPA Act relies heavily on GDPR principles of legitimate purpose, proportionality, and transparency, among others. Under PDPA controllers 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 (clients) 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 and personal information protection impact assessments.

3.2.5.2.2 General Privacy Principles

A core privacy principle is to only collect personal information that it is absolutely needed for a program to meet its objectives. A privacy risk review should scrutinize each piece of information by asking why it is needed – personal information should never be collected without a clear purpose. By avoiding collecting personal information unnecessarily, many inadvertent privacy risks can be avoided. Quite often information can even be collected without identifying individuals – this should be done where possible, and this also helps to avoid privacy breaches.

Another principle is the limitation of use, i.e., personal information should only be used for the purpose for which it was collected. The collection and use of this data must be clearly disclosed to the individual and their consent should be obtained where practical. Situations where personal information is used inappropriately for a secondary purpose or in a way that is contrary to the reasonable expectations of the individual should be avoided.

Programs should limit disclosure and avoid sharing of personal information collected about individuals. In situations where data is being shared, it should be clearly declared exactly which information is being shared, for what purpose and with whom it is being shared. Where practical, consent of the individual should be obtained. Unauthorised use of personal information may occur when clear guidelines are not established regarding the use of personal information. It is recommended that parties sharing information create data sharing agreement to document these terms.

Another core privacy principle is to only keep information for as long as it is needed. Clear guidelines for minimum and maximum retention periods and statements about individual programs should be established for the initiative that is collecting personal information around how long that data will be retained. A procedure for the notification of the end of a retention period and the secure destruction and verification of the deletion of the data should also be established, including electronic and paper copies and any backups or duplicates in existence (disaster recovery sites, etc.). Automation may be leveraged here in certain cases to ensure timely deletion. Periodic spot-checks should be performed to ensure that data retention procedures are being followed. Personal information that is not disposed of properly may be accessed without authorisation and may lead to a privacy breach.

To understand and communicate the potential privacy impact that a new digital health system may have, industry best practices call for a Privacy Impact Assessment (PIA) to be conducted. A PIA is a risk management process which assists in identifying and managing the privacy risks arising from the implementation of a new system. It helps institutions ensure that they meet any legislative requirements and identifies impacts that the new system may have on an individual's privacy. This PIA process benefits the stakeholders of the new system in many ways, including reducing the risk of unauthorised collection, use, disclosure, retention, or disposal of Personal Information. A PIA can never eliminate such risks altogether; however, it can help to identify and manage those risks. A PIA is not:

- a superficial legal checklist
- a one-time exercise
- a tool to hide risk and only show benefits of a project
- a justification for sub-standard policies or practices
- unnecessarily long, complicated, or difficult to read and understand

A process and framework should be established for conducting a Privacy Impact Assessment (PIA) for any health program that is considering or implementing a Digital Health System. A standardized PIA Template should be established for consistency and efficiency of conducting the PIA process in Sri Lanka.

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 should support 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:
    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.

Currently, aggregated data is captured from digital health solutions and reported via the eIMMR (electronic indoor morbidity and mortality register). This is an example of direct reporting of indicator values from health institutions.

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 staff members, ensuring that communications between staff, staff and patients, or administrators is stored in a manner which can be protected and monitored. Additionally, the establishment of a ministerial e-mail account for users ensures allow-listing of multi factor authentication (MFA) and other security notifications can be attained since they use official domains[25].
- 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.
- 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) 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, during capacity shortages or issues during public health situations. Service discovery of other facilities and organisations, allowing

[25] National Digital Health Guidelines and Standards [2] Section 5.3

for the future specialisation of hospitals and smarter deployment and mobilisation of resources (i.e., specialised paediatric hospitals or long-term care 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 care settings either. There are chronic and communicable disease use cases where the integration of information between disease programs would provide a high degree of benefit.

- 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)
- Integrating curative care records 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 those responsible for HIV care, or general practitioners)

3.3 Proposed Future State

The solution proposed to fulfil the needs of the DHP in Sri Lanka are illustrated in Figure 10. This desired Future State architecture provides a scalable framework for the solving of multiple digital health problems across domains, organisations, and care settings in Sri Lanka. The architecture describes a platform that should be constructed incrementally over time (i.e., Transitional States), as resources become available, and may take up to a decade to become fully realised.

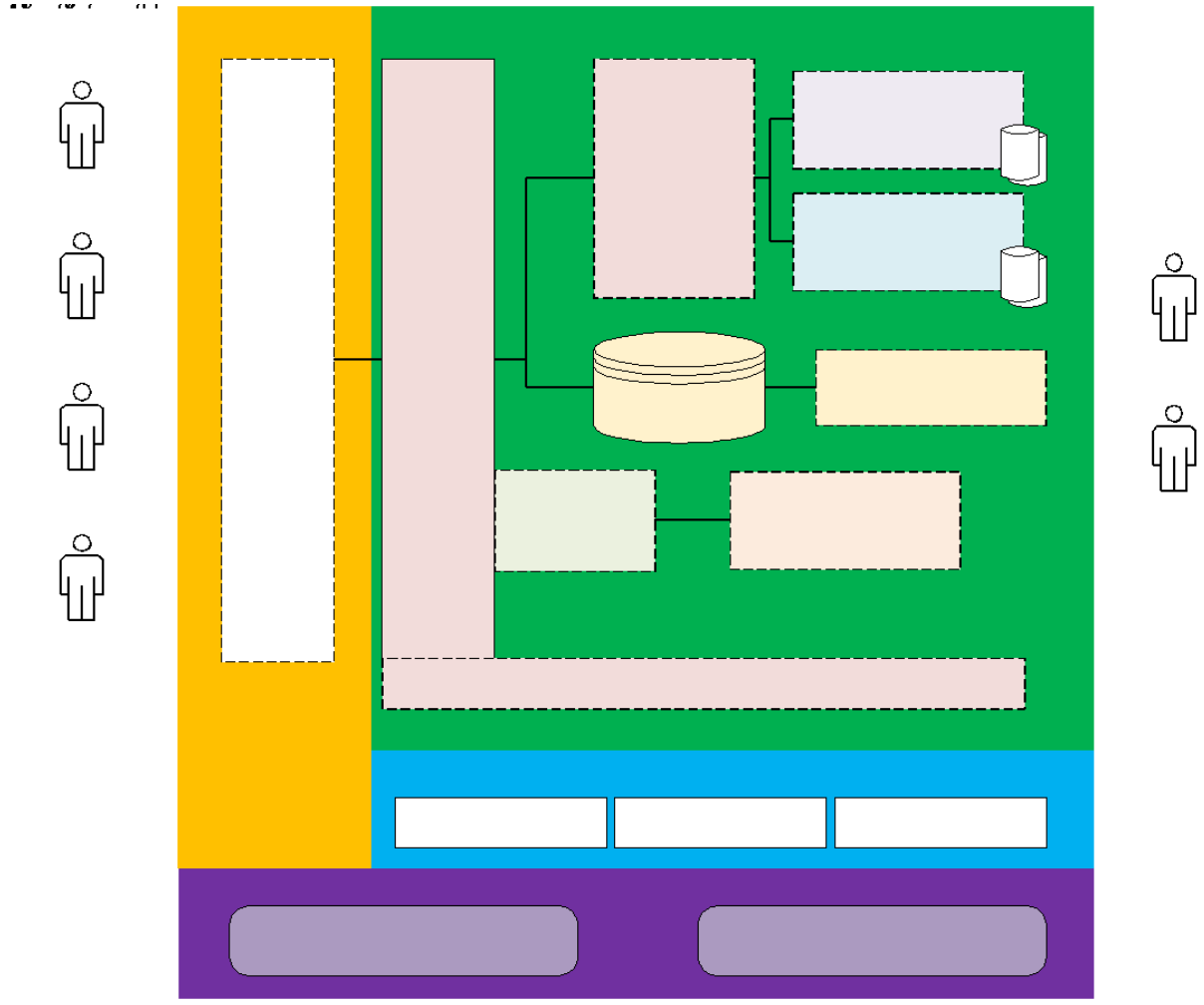

Figure 10 – Proposed Future State Architecture

The solution allows for the solving of problems by establishing systems into “points of service” applications, which consume and contribute data to a centralised infrastructure. These points of service solutions include any solution used directly by care providers (such as BHTs, EMRs, hospital systems), patients (personal health records, viewers, etc.) the general public (informative websites, public health sites, etc.) and administrators (HRMIS, planning tools, transfer and capacity planning, etc.)

The National Health Data Exchange (NHDX) provides common, shared services for the entirety of the enterprise including communications, message translation, mediation, orchestration, service quality, discovery and metadata exchange and abstraction of components of the broader health enterprise. The national health data exchange may use the National Data Exchange (NDX) as the foundation for integration within the health context.

The *shared infrastructure services* provided by the health data exchange will leverage common security services which are common to the entirety of the DHP. These services include encryption support (certificate management), authentication of devices/applications/users, auditing, and accountability tracing, SIEM (Security Information Event Monitoring), and privacy/consent management.

Data related to the administration of health services (both curative and preventative) are encapsulated by the functions of the *Health Administration Registries*. These registries are primarily concerned with the identification of facilities, providers, patients, materials, organisations, and other supportive data. The primary goal of these registries is the unambiguous identification of supportive objects in the NEHR. Functions in these registries may include governance, resource and workflow management (for approvals, issuance of identities, etc.), de-duplication services, and linkage services.

The information captured as part of a patient's NEHR is stored in one or more repositories of information (pharmacy data, lab data, imaging data, etc.). These repositories collect the relevant health events (referrals, discharges, admissions, procedures, etc.) which occur during the lifetime of a patient. Repositories are also responsible for enforcing appropriate data protection instructions (policy enforcement), performing any specific business functions (clinical validation, issue detection, etc.).

These repositories and registries are coordinated via *coordination services*. These serve as a type of "index" or table of contents for the DHP data and provide longitudinal linking, workflow and aggregation services. The repositories and coordination of links between the repositories and registries support the delivery of health between points of services in Sri Lanka.

Operational support systems are also included in the DHP diagram and represent support systems for MOH staff such as document management functions, knowledgebases, enterprise assistance (helpdesk), project management, ERPs, electronic mail services. While not directly integrated with the clinical data domain, these operational support services should still use common elements of the DHP including security services, authentication, and monitoring.

Finally, secondary use functions are supported by the Digital Health Information Warehouse (DHIW) which is used to store and disseminate KPI definitions and measures. DHIW data is populated either using an ETL patterns from other services in the DHP (example: number of encounters by month, number of positive HIV tests, etc.), real-time processing of metrics from the NHDX (example: active hospital admissions, transplant donor monitoring, etc.), or direct report from points of service (example: number of planned outreach sessions, monitoring of cold chain equipment, etc.).

The information from the DHIW may be used for secondary use purposes such as national dashboards, international reporting, research, and education development, etc. These secondary use services may directly be directly derived retrieved from the DHIW (example: dataset extracts, in-software dashboards, etc.) or accessed via the NHDX (example: if an HIS wishes to compare its internal KPIs with national KPIs).

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 all 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

When considering a solution to the complex domain of health service delivery, it is important to reduce the complexity into more manageable pieces of functionality. The blueprint proposes a services-oriented architecture (SOA) approach to mitigating complexity. The process of solving problems using a SOA approach is illustrated in Figure 11.

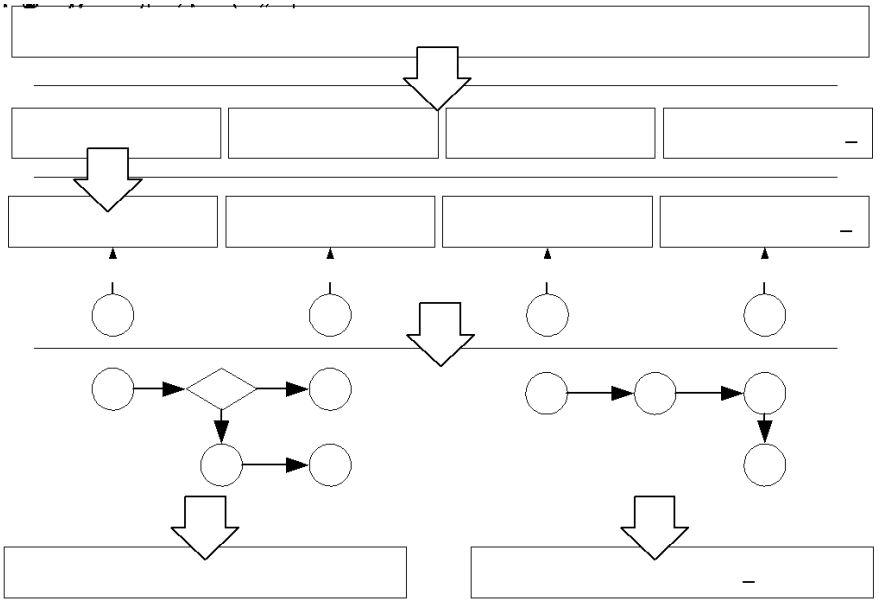

Figure 11– Solving Problems using a SOA Approach[26]

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.

3.3.2.1 Enterprise Services Design

Careful consideration should be taken in the design of the services described above, specifically when it comes to the granularity of the services. Figure 12 presents the spectrum of choices considered when designing services.

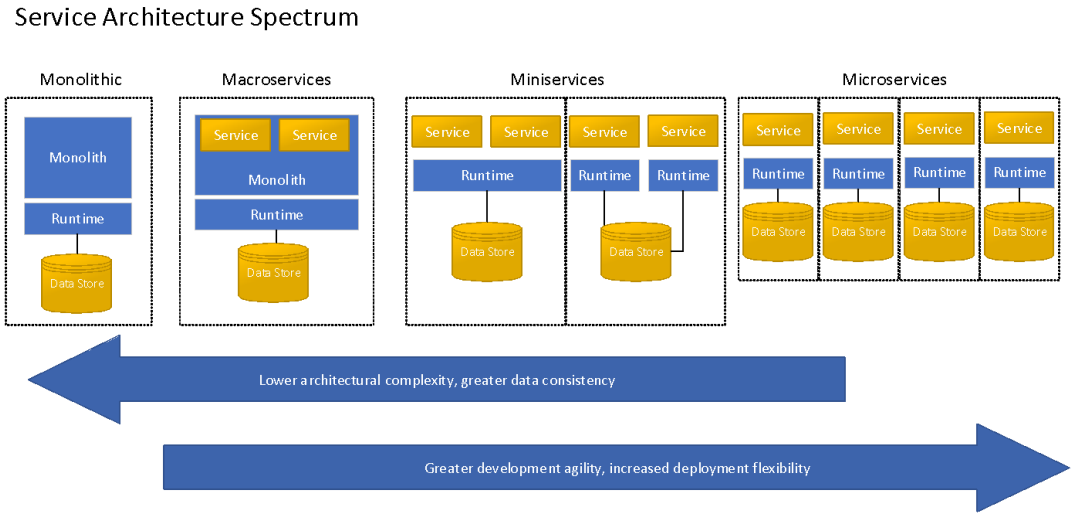

Figure 12–- Services Architecture Spectrum[27]

There is no consensus on an approach to determine the exact level of granularity for a service. Services that are dedicated to a single task are referred to as atomic services. Composite services may call many atomic services to achieve a more complex task.

[26] Adapted from: Erl, Thomas – SOA Principles of Service Design, ©2008, Prentice Hall ISBN 0-13-234482-2
[27] Adapted from Gartner Research Webinar Series https://www.gartner.com/webinar/3437517

For example, consider a software service which handles electronic referrals (e-Referrals) between facilities. Such software would need to provide functions to register/resolve the patient, register/resolve the facility, as well as manage the data and status of the referral itself.

An implementation of this could be achieved using any of these design patterns:

- *Monolithic:* In a monolithic implementation, a single application provides the “refer patient to facility” functionality (via API or UI). This software solution would handle all registration of patient data, validation of facility services, provider lookup and scheduling before inserting the necessary data into a single database. There is no opportunity to perform functions beyond that in the single application.
- *Macroservices:* In a macro-service implementation, a single software solution with a single database may provide multiple service APIs which can be invoked by callers to perform the e-referral. This may include one or more services to find/create patients, find the facilities, find providers, etc. The caller would invoke these services on the single runtime and a single database. This provides a high degree of referential integrity and a lower operational footprint as well as consistent business logic between services. However, the reliance on a single software solution increases application development complexity, and regression testing complexity.
- *Miniservices:* In a mini service pattern implementation, one or more services are provided by one or more runtimes with multiple databases. For example, an MPI service would provide only those functions related to patient registration, de-duplication and resolution, whilst a facility registry service would provide only those functions related to facility registration. The caller would invoke these services to resolve patient and facility information before submitting the referral to a referral service which may validate this information. This allows for a degree of referential integrity within a particular service (the MPI remains consistent) and separation of concern between services based on business function, and still permits a higher degree of service composition. The pattern does introduce a higher degree of operational complexity (as there are multiple services which need to be operated) and links between these mini services can degrade over time.
- *Microservices:* In a microservices pattern, services are separated by their functional role, and APIs are exposed at a CRUD level (create, update, read, delete) for resources on that service. In this example, a patient microservice would expose CRUD operations for patients, and a facility microservice would expose CRUD operations for facilities, and a referral service CRUD operation for referrals. The coordination of these services is entirely at the discretion of the caller (i.e., the caller must compose these services to meet a business objective). Services are intended to be atomic and provide only one small unit of functionality. This reduces the complexity of maintaining the service application code at the expense of lower referential integrity, lower consistency of processes (as the caller is responsible for coordination) and higher operational complexity.

The benefits of using smaller services include increasing modularity, making applications easier to understand, develop and test relative to monolithic architectures. Smaller services also improve scalability since microservices are implemented and deployed independently they can run within independent processes and can be monitored and scaled independently. Smaller services also enable more distributed and parallel development process by enabling teams to develop, deploy and scale their services independently.

The main drawback of making services too small and/or only using a microservices approach is the large runtime overhead and operational complexity that is introduced as services become smaller. Some additional drawbacks of using smaller services include application performance, as small services tend to have a much higher cost in terms of network latency (http overhead, decryption, etc.) and message processing time than in-process calls within larger services or a monolithic service process. Testing and deployment of many small services can become laborious and complicated. Refactoring and moving responsibilities between services can become difficult with smaller services as multiple services are impacted and therefore multiple teams require coordination.

The coordination of distributed state change (for example two-phased commits) results in a tighter coupling of all the participants within a transaction. Services that are too small can create awkward processes which have to be implemented by transaction participants to maintain data consistency.

Overly small services and the use of many separate data stores can create challenges with data aggregation. To have a full view of a working system, data sets must be extracted from many microservices repositories to be aggregated into a single schema. For example, it is often not possible to create operational reports using a single microservice repository.

Mini services have emerged as a simpler, pragmatic way of doing microservices applications primarily due to lower overhead and the fact that mini services may share data in a single datastore with referential integrity enforced at a database level. In general, the best balance of benefits and drawbacks on the spectrum is to prefer the use of mini services, however it is important to understand that any choice of services architecture does not fundamentally remove complexity from a system design, it just moves the complexity from place to place.

Because of these factors, the blueprint proposes that digital health services for the DHP follow mini-service and macro-services patterns. These services will be designed in the solution views along business objectives (i.e., register discharge summary rather than create observations API). The use of microservices at the DHP level (i.e., microservices via the NHDX) is discouraged for data update or create operations.

3.3.3 Interoperability

The goal of establishing a NEHR for all patients 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-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[28].

Work has already been performed in the National Digital Health Guidelines and Standards (NDHGS) document to establish baseline interoperability guidelines. These will be extended and elaborated upon

[28] Interoperability in Healthcare | HIMSS

in a forthcoming interoperability plan. At a high level, interoperability within the proposed solution of 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 Standards and Guidelines [2] sets forth guidelines for the data elements to be captured by digital health solutions. These elements should be adapted and referenced in solution 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.
- *Behavioural 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[29]. 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[30] which can be applied to enterprise integration environments. Using the services-oriented 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.
- *Geographic Scalability*: The ability of the DHP and its services to grow to support new geographic regions and their related governance and access requirements.

[29] LIFe - Lanka Interoperability Framework

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

- *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 design framework specified in the blueprint (and by extension the implementation in the DHP) separates the conceptual (enterprise view), the logical (solution or business view) and physical (technical view). This pattern should be followed for every service implementation within the DHP.

The separation of these views ensures that the DHP can support new technologies 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 becomes available (HL7 Version 5 for example), the same business functions can be realised in this new standard.

Additionally, the use of an enterprise 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 (for example) 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 may be required and the DHP should permit the onboarding of these technologies.

3.3.4.2 Geographic Scalability

The DHP is designed as a series of services linked together via interoperability standards on an information exchange. By leveraging this design pattern, it is possible to establish cross-community access of information between realisations of these exchanges, or services within the DHP.

This is important since the DHP must operate in a manner which permits sub-national registration / governance of services, users, and data. Common use cases for this type of scaling are:

- Sub-national jurisdictions (regions, provinces, institutions) may onboard/restrict access to software which operates only within their own province without the need to apply to the central level for access certificates.
- Sub-national jurisdictions may manage access credentials for users which they have hired without the need of central administration doing so.
- Sub-national jurisdictions may manage their own reference lists for facilities, patients, providers, human resourcing as appropriate, according to their own environments without the need of central administration.
- Sub-national jurisdictions should be able to define and approve their own indicators without the need of central administration.

- Sub-national jurisdictionally granted access (either signing certificates, user access credentials, etc.) should be isolated from central access. This isolation should mean that provincially issued credentials and certificates are not inherently trusted by other provinces or the central system, however centrally issued credentials and certificates are trusted by all provinces.

The DHP does not prescribe the way this form of functionality is attained; however, federation is a useful construct to obtain these abilities. Federation can occur at the data exchange level (see Figure 13), at the individual service level (see Figure 14) or can be an inherent property of the digital health service software implemented within the DHP (or a hybrid of these models).

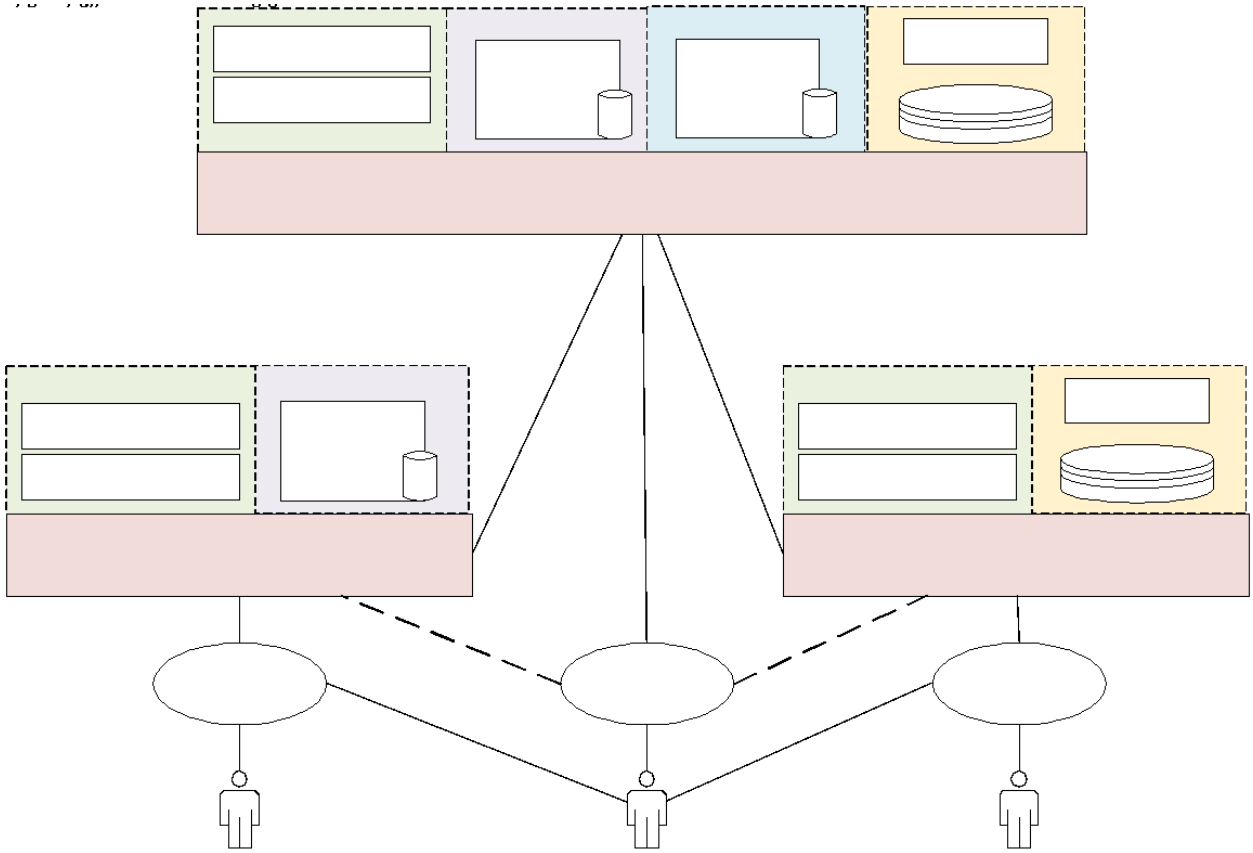

Figure 13 - Federation at Health Exchange

Figure 13 illustrates a scenario where two provinces exist as child exchanges (or communities in IHE parlance) to a national community. The attributes of the health exchanges are:

- National: Contains the shared infrastructure relevant to centrally managed databases, indicators, security credentials, provider registration information, etc.
- Province 1: Has authority to issue and revoke provincial access certificates, identity credentials and has established its own provider registry.
- Province 2: Has authority to issue and revoke provincial access certificates, identity credentials and has a provincial information warehouse with its own KPI definitions.

In this model, Province 1 may issue its own device authentication and digital signing credentials (via its own provincial intermediate authority) to its own trusted systems, as well as its own user credentials to a provincially hired nurse. Since the provincially issued certificate for the pilot system is not trusted by the national data exchange, it won't be able to access or sign data to that level in the hierarchy. Additionally, the provincially hired nurse will not exist in the national provider registry (requiring no approval centrally to create new provider records) and will not have access credentials to query systems (since the national IdP did not issue the credentials)

Province 2 may also issue its own certificates for its own software solutions, and user credentials for its own users. Any custom reporting and data collection requirements can be managed by the province.

National certificates (issued by the Sri Lanka national CA) and national credentials (issued by the central IdP) can be used to access data on the central digital health infrastructure, or on the provincial health infrastructures (since there should exist one-way a trust relationship).

Federation of data at an exchange level provides several advantages such as data isolation (provincial authorities can turn off access rules if required), establishing a local network of trust (where provincial users can only access provincial data within their own tenant).

The cost of this is complexity in running multiple tenants, and the necessity of having a separate provincial support structure.

An alternate model of federation is to federate individual services within the central digital health platform (see Figure 14). Whether this is done at an instance level (i.e., the software is separated on provincial tiers) or at a data level (i.e., the data is logically separated and controlled via access rights), the logical behaviour should be similar, however at the cost of isolation of data and services between communities.

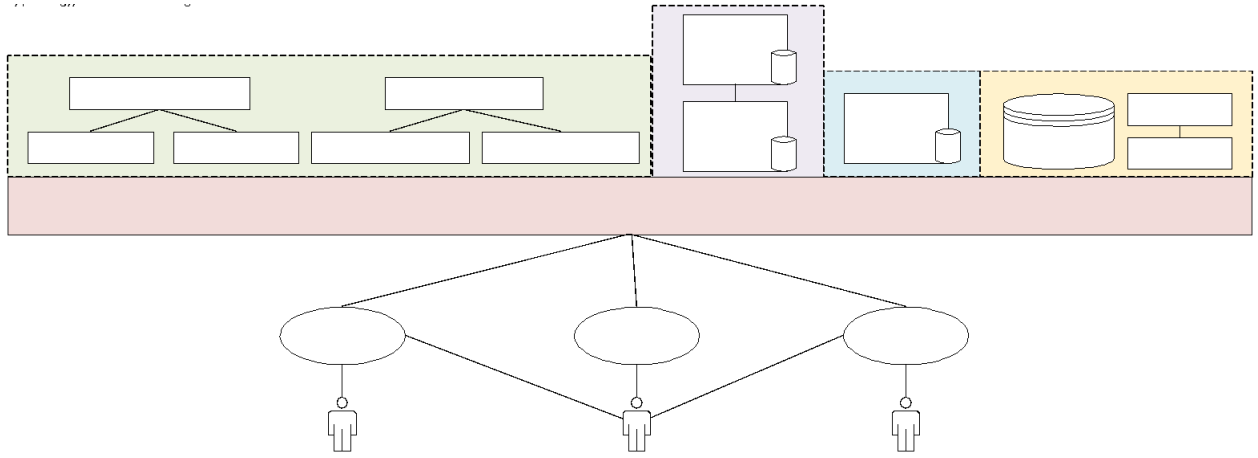

Figure 14– Federation of Services

3.3.4.3 Heterogenous Scalability

The underlying foundation of the proposed solution is based on an open architecture[31] which permits the scaling of the DHP over time within a heterogenous manner by defining the behaviours and interfaces in a standard manner. This means that components of the DHP and consumers of DHP data may be implemented and realised by a variety of vendor solutions with no impact on the functioning of the DHP.

Solutions may be open source (preferred) or proprietary (free or commercial software), written in any language on any operating system and should operate comfortably within the DHP. 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 the onboarding and growth. By using open architecture and specifications, new organisations and users may be onboarded to the shared DHP infrastructure without impacting existing organisations or users.

The administrative burden of onboarding a new organisation should involve little more than registration of the organisation's certificate (public/private key pair) to access NHDX services and setting appropriate application credentials on the shared identity provider. New users, similarly, may be added with their official e-mail addresses and granted a credential on the identity provider.

Additionally, the use of standards-based interfaces means that developers and operators of points of service solutions may easily understand and adapt the NEHR and other DHP services to meet their needs without "one off" scale up.

Finally, 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

The definition and separation of services within the DHP along their business objectives, combined with the use of SOA ensures that the solution is functionally scalable. Functional scalability ensures that new operations (or functions) can be added to the solution without impacting or changing other functions.

The DHP achieves functional scalability by encouraging:

[31] 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.

- *Encapsulation*: Each service and exposed by the DHP, should expect to receive from any source, all data and trigger event information required to perform the desired business function. There should be no assumption that a target service or eventual consumer of data "knows" information not included in the original payload. This ensures that different implementations of the service can be "swapped out" with another implementation or removed completely without impacting the operation of other services in the DHP. Furthermore, each service should store and faithfully reproduce data which it has received. There should be no assumption that the caller will have access to other services, or that referenced data is readily available. For example, a submission to the NEHR repository should include the details of the sending organisation (such as names and business identifiers) without assuming the NEHR repository can "figure out" such data based on a simple UUID or URL.
- *Loose Service Coupling*: Each service within the DHP is loosely coupled. Loose coupling means that each service does not have hard dependencies on another within the DHP or outside of the DHP. Loose service coupling ensures that if a function of the DHP is missing, replaced, or deprecated, that other services may 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 rationale for dividing the health enterprise into domains is to reduce the large problem of enterprise integration into smaller, easier to specify areas of concern. It also allows the blueprint to organise the business function of service, and to articulate the impact the DHP will have on each.

The business domains referenced in the blueprint are:

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, monitoring activity within the DHP, encrypting and signing data, special consent directives and more.
3. *Health Administration*: Concerned with the administration of health services. This problem domain encapsulates the identification of locations, providers, clients, supplies and logistical support.

4. *Health Delivery*: Concerned with delivery of curative and preventative clinical care. This problem domain encapsulates functions related to record location, indexing, storage/retrieval, and non-repudiation across clinical domains.
5. *Operations Support*: This domain is concerned with the overall operation and delivery of care for the Ministry of Health and related stakeholders including helpdesk, communications infrastructure (e-mail, SMS, etc.) and dissemination of procedures and policies (knowledgebases)
6. *Secondary Use*: This domain is 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 DHS.

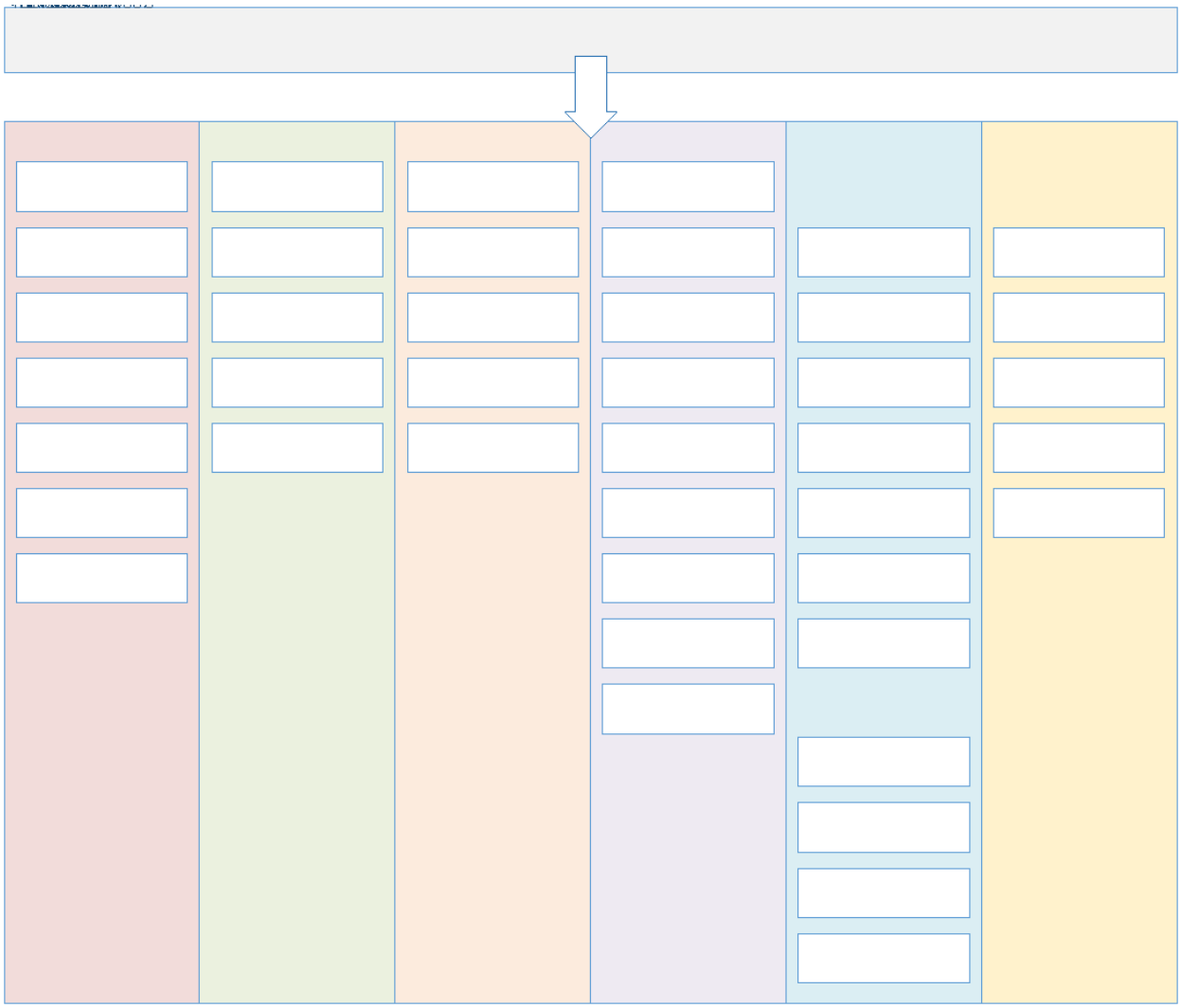

Figure 15– Business Domains and Functional Concerns of the Blueprint

3.3.5.1 Shared Infrastructure

The shared infrastructure business domain of the blueprint business architecture is primarily concerned with the technological infrastructure of the DHP. Shared infrastructure primarily concerns itself 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.
- Integration services related to the transformation of messages (where appropriate), orchestration of enterprise flows (where appropriate), and publish and subscription services (i.e., enterprise service bus features).
- 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.
    d. Governing the linkage and resolution of patient, facility, provider, and consumable identities in a manner which ensures that data within the enterprise is not corrupted or altered by systems which ought not update these types of data (i.e., a district hospital is not permitted to merge PHN numbers).
- 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.

3.3.5.2 Privacy and Security

The privacy and security domain is concerned with ensuring the security of the entire DHP is maintained and that patient privacy consents are documented and enforced. The primary business functions provided in the domain of privacy and security are:

- Certificate management services which are used as the basis for cryptographic digital signatures, node authentication, and encryption in transit and at rest. Certificate management is important for ensuring security of information in transit and at rest.

- Common authentication services, which are used for ensuring that each digital health service within the DHP is aware of the user, application, and device identity of the source of information. This is necessary:
    a. To implement enterprise-wide policies between systems,
    b. Identify end-users and applies policies within the digital health services (for example, a repository of HIV lab results may impose specific privacy constraints based on the user requesting the data).
    c. Reducing duplication of logic across the enterprise (password management, one-time-passwords, revoking access credentials, etc.)
    d. Simplifying access to systems by providing consistent patterns and credentials for access
    e. Role based access control
- Consent tracking services, used to track the opt-in or opt-out of a patient in a particular data programme. For example, a consent directive by the patient that their medical records may be used on their death for research purposes.
- Common auditing services which are of vital importance to accountability tracing of users, devices and applications connected to the DHP. Auditing services provide the basis for making administrative decisions about users, and the detection of security breaches.
- Consistent timestamping services: In any enterprise where, multiple systems are submitting data on a variety of different hardware devices, in different organisations, it is important an "official time" be maintained between actors in the system.

ICTA, Hospital IT staff, and MOH are the primary drivers of the privacy and security domain. The privacy and security business domain of the Sri Lanka DHP provides fundamental services which should be leveraged by all other business domains.

All connected points of service, digital health services, and other custodians of health data (those organisations, private or public which store or use health data) are expected to pass conformance testing prior to being issued access credentials to the DHP. The technical and information principles which all connected services are expected to abide by are outlined in sections 6.2 and 5.2.7 respectively.

3.3.5.3 Healthcare Administration

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: The administration of client demographic data within the DHP is of the utmost importance. The health administration domain supports the rest of the delivery of care by providing consistent, unambiguous identification of patients who are seeking care or for which there is data submitted to the DHP, although by de facto, identification is never a prerequisite for care provision in Sri Lanka
- Identification of Provider Workers and Organisations: The identification and administration of providers is important within the context of the DHP. Identification of providers within the enterprise should be concerned with reliable, unambiguous identification of providers of care, and their services provided.
- Identification of Facilities and Services: The identification and administration of facilities and the services which they provide is a key component of health service discovery within the DHP. This

function facilitates the unambiguous identification of a service delivery location of care within the DHP, as well as allowing for future use cases of searching via services offered at each facility.

- Human Resources Management: The assignment and management of medical officers, nurses, clinicians and other support staff within the public sector are a concern of the health administration domain. The use of human resources data is informative to the DHP.
- Terminology: Consistent definition of concepts and their mapping to standard terminologies within the DHP is required for consistent identification of concepts (including those related clinical aspects) used between systems. Terminology services typically provide services for validation, translation, mapping, approval and retiring of terms used within the enterprise.
- Logistics Support: The unambiguous identification and description of devices, materials (such as syringes, scalpels, etc.), drugs and medications, vaccines, etc. it vital for establishing semantic interoperability between systems. This function within the blueprint is encompassed under the health administration domain.

3.3.5.4 Health Delivery

The health delivery domain is used to describe the business concerns within the DHP related to the delivery of care to patients and supporting transactions.

This domain is often classified into services provided for curative purposes and those provided for public health. The patient centric nature of the patient's NEHR, however, means that within the shared records infrastructure for health delivery, there will be no concrete delineation between these types of data. A patient's NEHR may contain public health information related to immunizations, quarantine, and communicable disease diagnosis as well as information related to hospital admissions and discharges.

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

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 admissions and discharges to/from hospitals, encounters/visits, chronic problems or concerns, allergies, patient preferences etc. The DHP does allow for a single structured clinical data repository, however this is not assumed since new technologies, heterogenous content (like PDFs, DICOM WSI images, digital pathology systems, and genomics) will exist in the future. The term "clinical data repository" is understood to mean any repository of clinical information directly related to a patient.
- *Decision Support Services*: Which are used to provide clinical decision support to users by proposing actions which may occur to adhere to a best practice, or clinical protocol. Decision support services can simply be informative (i.e., an obesity screener) or they can be used to derive care plans (i.e., vaccination schedule, cancer care plan). Decision support services ingest a series of configured rules and apply these rules against a set of data (or facts).
- *Care Guideline Repositories / Clinical Knowledgebases*: The job of storing, managing, and versioning (including retiring) best practice and standardised care guidelines is also under the purview of health delivery. These guidelines may be computable in nature (i.e., used by decision support services within the DHP or downloaded by PoS applications), but may also be narrative descriptions.
- *Inventory and Logistics Services*: The digital capturing, management, and reporting of current stock levels to the DHP is useful in predictive stock management (i.e., preventing stockouts using machine learning) as well as balancing facility load based on availability of stock. Additionally, health delivery facilities and supply chain management solutions may interact using non-health standards (GS1 Business Messaging Standards) to manage the order request/response, despatch, arrival, and acceptance workflow.

This business domain primarily supports the frontline provider workers in the delivery of quality care, and central/provincial ministries of health in evaluating adherence to and implementation of policies.

3.3.5.5 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 business domain within the DHP is used to describe services which the MOH and ICTA provide, which can leverage the shared security infrastructure, however, are not related to care for patients (rather the organisation of the resources which provide care to patients).

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. This can be used for CPD programmes. 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. A well organised LMS can be used to disseminate training materials as well as track compliance and certification.
- 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. Additionally, such solutions can be used to disseminate downtime information to a broad audience of system operators.

- Enterprise Knowledgebases are important for documenting new policies, circulars, software features, interoperability standards and standard operating procedures. These knowledgebases are typically indexed and allow staff and users of points of service solutions to quickly find information about the DHP.
- Document management solutions are important for the workflow and management of policy, circular, technical, or public documentation whilst maintaining a complete set of version history for documents.

These operational support systems won't necessarily use the NHDX, or clinical infrastructure within the DHP, however they should use the common security infrastructure. Many common off the shelf (COTS) solutions should be compatible with:

- E-Mail and SMS notification gateway servers for sending alerts to users
- Identity provider functions to allow users to use their DHP credentials to log into the LMS, DMS, etc.
- The certificate services used by the DHP for encrypting traffic and data at rest.
- Event monitoring software such as SIEM or APM

3.3.5.6 Secondary Use

The secondary use business domain encapsulates all functionality which uses clinical data for uses other than delivery of care. The electronic Indoor Morbidity and Mortality Register (eIMMR) is the primary example of a secondary use service currently leveraged within Sri Lanka, however other secondary use solutions exist for programmatic and monitoring purposes.

In addition to the current use cases for secondary data capture and use, the proposed solution considers additional uses of information in the digital health information warehouse:

- 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, and more
- Drug and device recalls, tracking where a particular drug or device has been used and needs to be recalled and/or replaced
- Geographic Information Systems (GIS) use cases for plotting coverages, wait times, service availability

Secondary use data can 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 as transactions occur within the crossing the data exchange whereby information events are sent to the DHIW as the event occurs. This pattern is useful for near-real-time indicators.
- 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.

The physical implementation of the health information warehouses within the DHP may include technologies including:

- Traditional relational databases using snowflake, Data Vault or other schemas defining data marts
- Big data patterns such as data lakes and data mining via ELT processes
- Online Analytical Processing (OLAP) cubes and related technologies

4 Application Architecture

4.1 Current State

The current state of the information systems and information flows in Sri Lanka is shown in Figure 16, which illustrates a high-level overview of existing health information systems and their interactions for context. The figure provides a visual representation of the systems in operation within Sri Lanka, and a classification of their role (the administration of health, the delivery of curative or preventative services, and supportive services) and whether they are centrally managed (i.e., in a cloud or web environment), or whether they are operated on-premises.

Most of the information systems operate within the preventative or curative area. Systems which are operated by government are denoted with rectangles, and private solutions are denoted in ellipse.

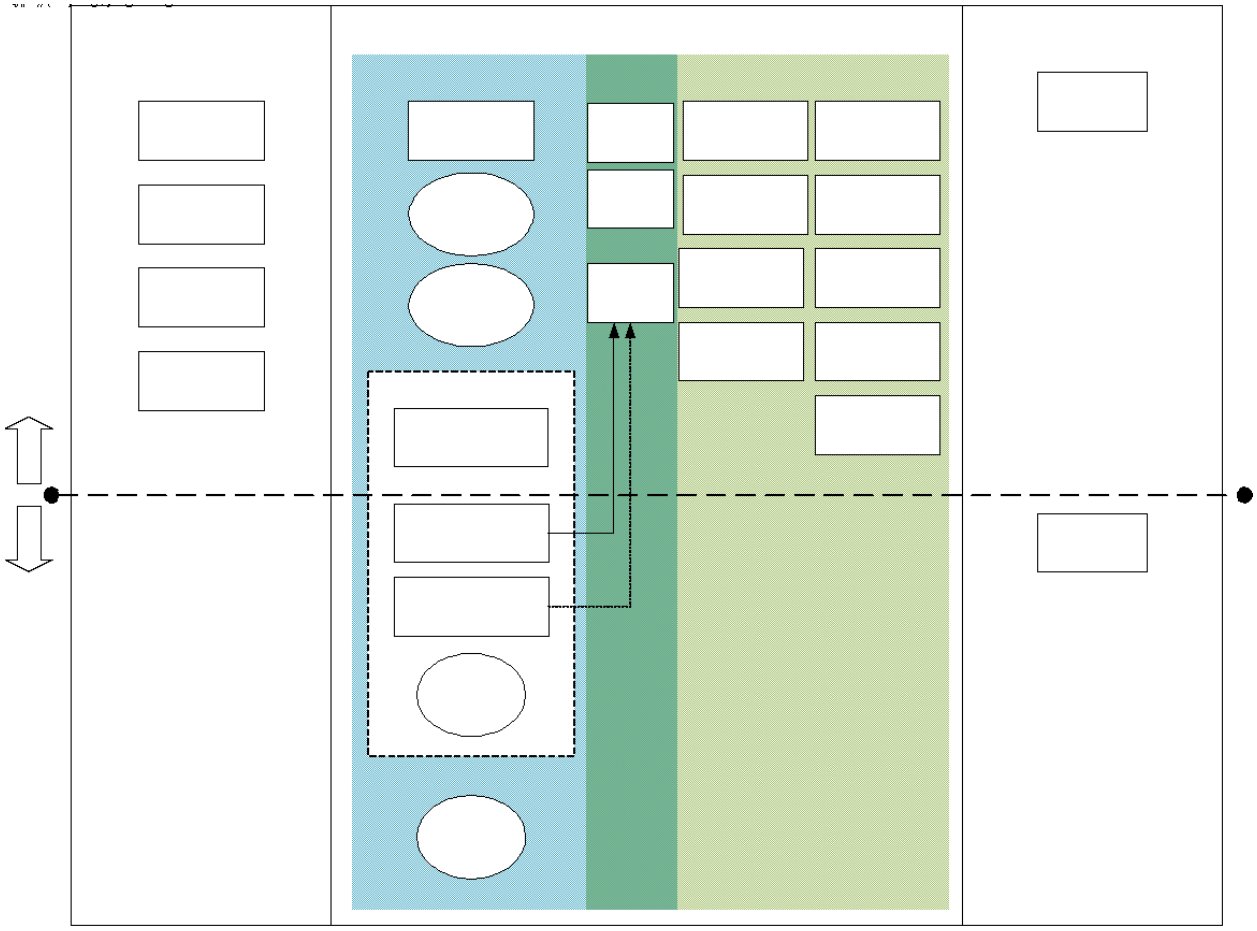

Figure 16 – Current State Conceptual Architecture

A complete list of abbreviations can be found in 0, however the abbreviations for Figure 16 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.

As shown in Figure 16, the primary information flows which are identified are from the HIMS and HHIMS to the Electronic Indoor Morbidity and Mortality Register (eIMMR). This information flow development should be considered for alignment with the DHP using a standardised reporting interface.

4.2 Proposed Future State

The proposed solution illustrated in Figure 17, is a refinement and further specification of the proposed architecture in Figure 10, on page 70.

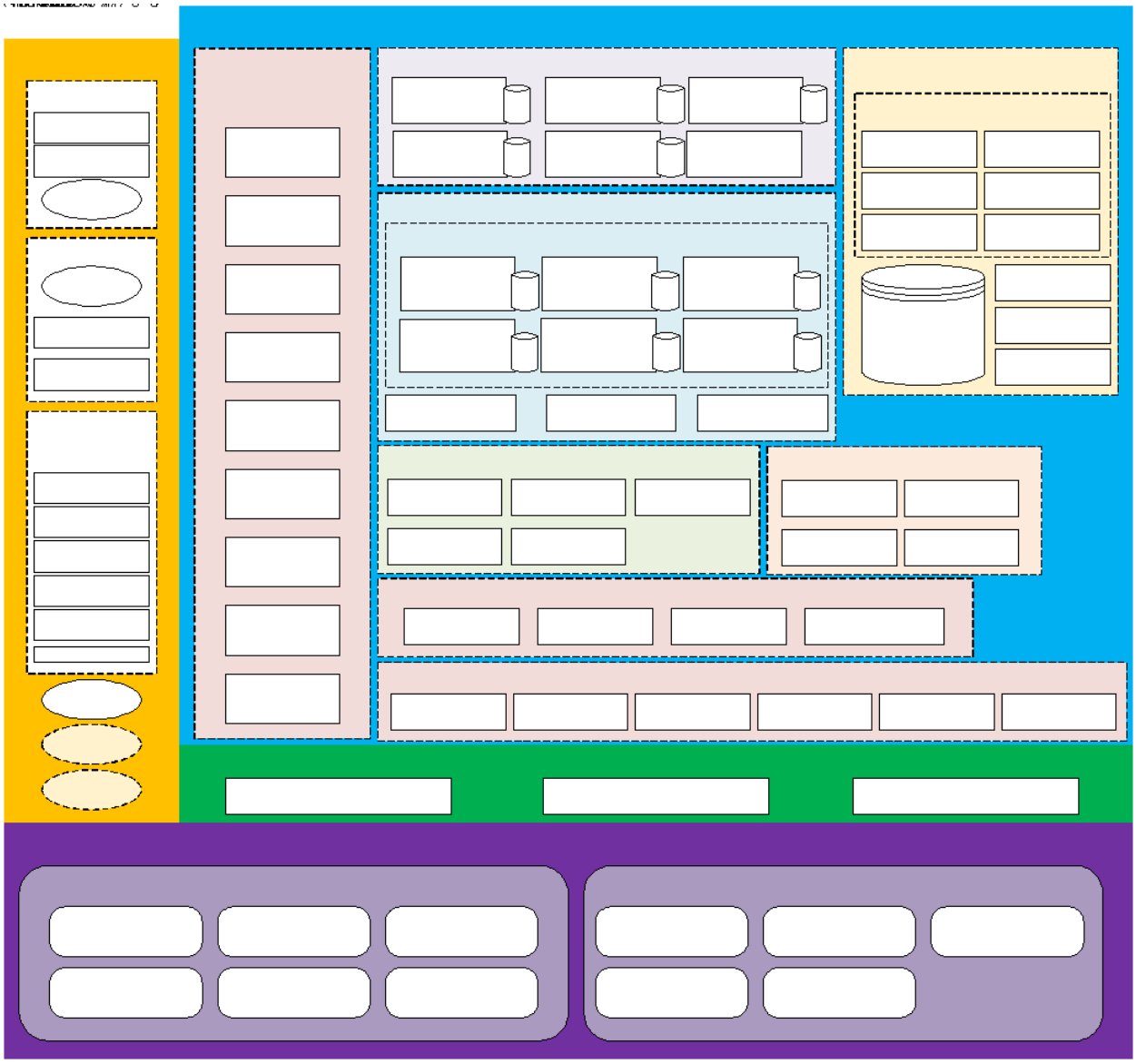

Figure 17- Conceptual DHP Architecture

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, a multiple software packages may work together as a single logical DHP component, or a single software package may implement multiple functional components.

For example:

- WebIIS may expose detailed immunisation information in FHIR and participate as a part of the Shared Data Repositories and as a Point of Service and as a Care Guideline repository.
- An insurance information system may act as a payment gateway service and a repository of financial transactions and insurance coverage.
- An Enterprise Service Bus (ESB) solution acting as the NHDX may provide messaging, mediation, business process execution, push notifications, logging, retry, load balancing and API access control in one solution. Alternately, a combination of an ESB for routing and mediation may be combined with a specialized API management solutions which together would act as 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. It is expected that implemented software services, legacy implementations, and software developed in the future (for example, 5 or 10 years from now) may use different standards, but still adhere to the same patterns and business services.

4.2.1.2 Infrastructure Diagrams

Diagrams in this section, and in the solutions views may 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 may be as illustrated in Figure 18.

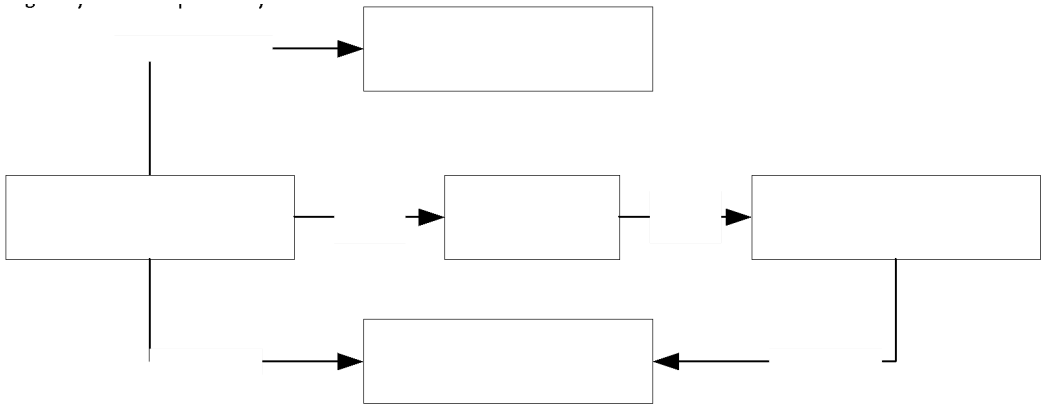

Figure 18- Actual Actor Relationships

However, documentation may use a simplified form as shown in Figure 19, 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.

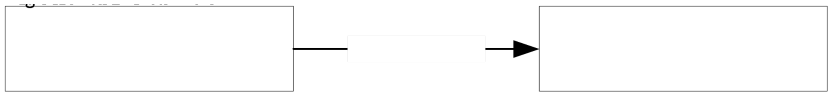

Figure 19- Simplified Actor Relationship

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 36). This section describes the general considerations of points of service applications within the DHP.

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 may become outdated.

4.2.2.1 Hospital Information Systems (HIS)

Hospital Information Systems in use in Sri Lanka include the Hospital Health Information Management System (HHIMS) which is used primarily to manage outpatient visits, and the Hospital Information Management System (HIMS) and an upcoming OpenMRS implementation which are used to manage inpatients. Both 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 may 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 HHIMS or Cloud HIMS). 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 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 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 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 (e-RHIMS), 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. Special purpose systems such as finance and logistics systems can be integrated with systems such as the immunisation system to provide efficiencies in supply chain management.

4.2.2.4 *DHP Viewer / Personal Health Record (PHR) Systems*

In the future, 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. For example, the following visualisation shows a future patient-friendly bloodwork result that could be available in the patient portal:

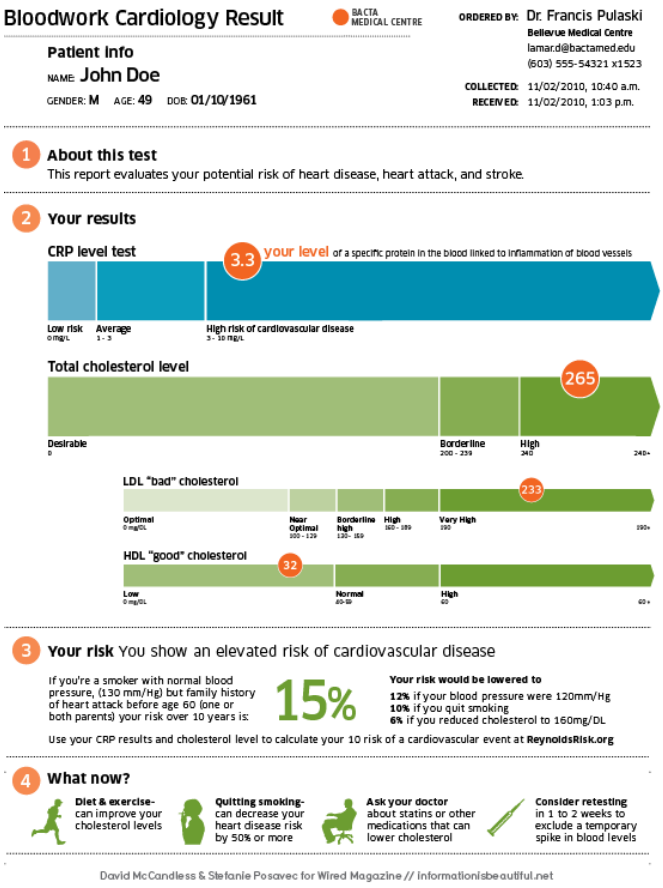

Figure 20 – Example Future Patient Portal Bloodwork Result[32]

[32] https://informationisbeautiful.net/2010/visualizing-bloodtests/

4.2.2.5 PoS-to-PoS Communications

In the future, clinical use cases may arise whereby direct information flows between points of service is desirable over registering long-term persistent data to a DHP service. For example, the routing of consultation notes between specific points of service.

When this need arises, points of service will use the services of the NHDX to achieve communications rather than relying on peer-to-peer patterns of exchange. Solutions running in the LGC or on the LGN and providing secured REST APIs act as both a "in front of the NHDX" and "behind the NHDX" service concurrently as illustrated in Figure 21.

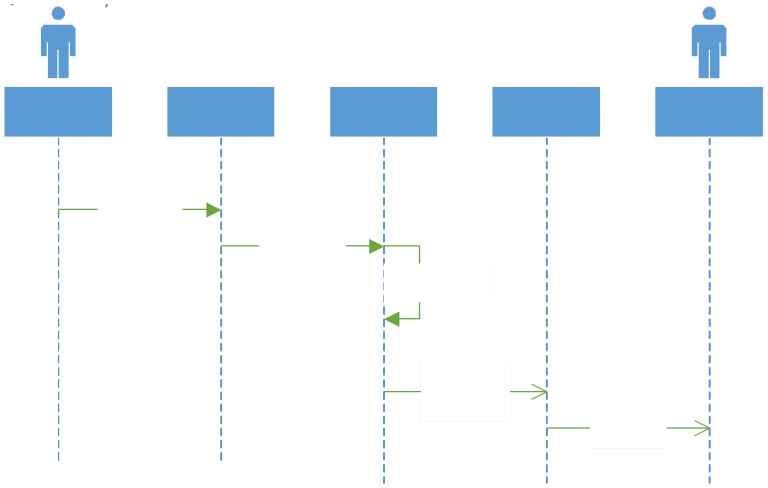

Figure 21- PoS-to-PoS Communications

The rationale for leveraging the common functions of the NHDX to facilitate PoS-to-PoS communication is:

- The NHDX can provide reliable delivery services (queue and retry on failure) to ensure that such data is conveyed to the target system without risk of data loss, especially important for facilities with unreliable communications connections.
- The access control, authentication, mediation, validation, resolution, and other services built into the NHDX can be applied consistently.
- Auditing and message logging services can be used within the NHDX to audit the transfer of information between the two points of service.
- Events which should trigger secondary use alerts, updates to the DHIW, or other subscribers within the DHP can be appropriately notified of the event.

4.2.2.5.1 Transfer of Large Data Objects

The PoS-to-PoS communication methodology can (and should) be leveraged for large binary blocks of data which need to be transported from care delivery settings. Examples of digital health information which consumes multiple gigabytes of information include:

- Digital Medical Images[33]

[33] DICOM Whole Slide Imaging (nema.org)

- Digital Pathology Images[34]
- Genomics Data[35]

Transferring such large quantities of data from the capture device to a central cloud location would be cost inefficient in terms of bandwidth and storage requirements. However, with the implementation of a Record Locator/Index service and inclusion of pointers to the source system which captured the image, it would be possible for the NHDX to point (or redirect) a client/consumer to the source with appropriate access credentials. Such an integration pattern may be executed in future revisions of the blueprint as illustrated in Figure 22.

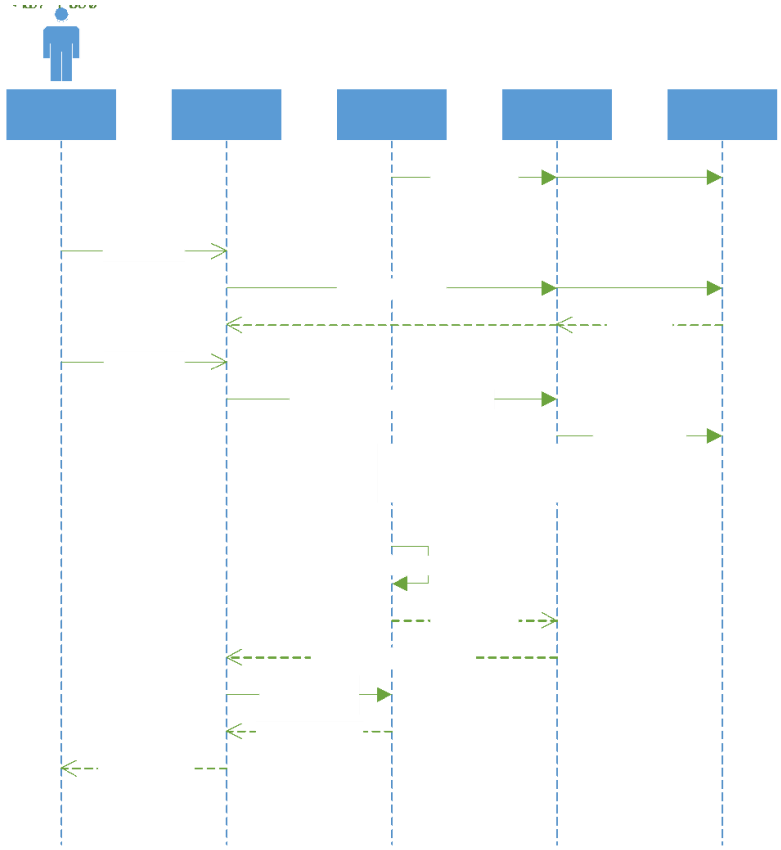

Figure 22- Transfer of Large Data Objects

4.2.3 Shared Infrastructure

The shared infrastructure domain is described in Figure 23 and specified further in this section. For reference, the components of the conceptual architecture included in shared infrastructure domain are illustrated in Figure 17.

[34] Comparative Assessment of Digital Pathology Systems for Primary Diagnosis - PMC (nih.gov)
[35] Storage and Computation Requirements | Strand NGS (strand-ngs.com)

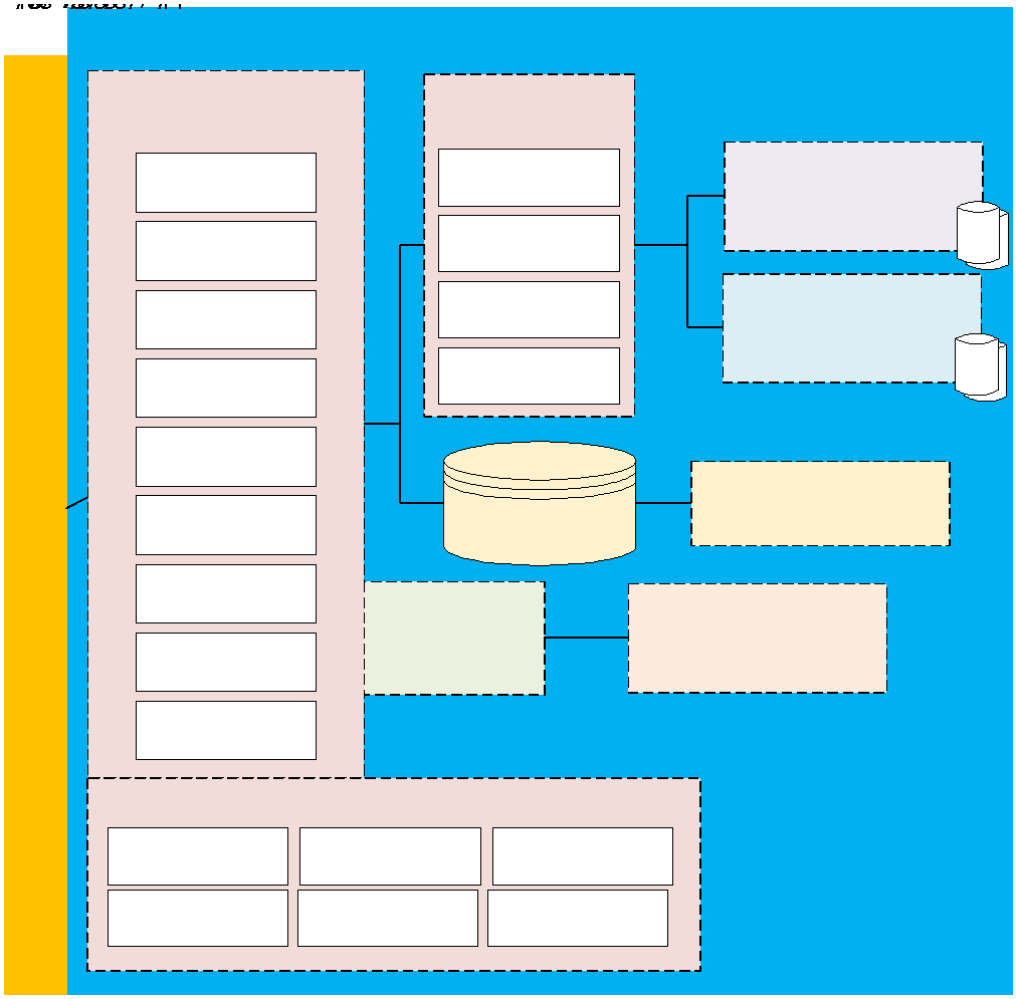

Figure 23- Shared Infrastructure Components

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 may be implemented with similar technologies used in the National Data Exchange (NDX) to reduce capacity building and training on a new platform. However, physically these would be different implementations. This is due to the scope of the NDX (exchange between ministries and programmes) differing from the NHDX (exchange of health data only) and the need to mediate data between these programmes.

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)

The messaging standards which the NHDX may be required to support include:

- HL7 Fast Health Interoperability Resources (FHIR)[36] for general purpose clinical data.
- HL7 Version 2 messages over secured Minimum Lower Layer Protocol (MLLP) where FHIR is prohibitive (such as integrating legacy or proprietary solutions)[37]
- IHE Aggregate Data Exchange (ADX) profile
- IHE Cross Community Document Sharing (XDS) using ebXML for sharing Radiology Reports, and other structured clinical documents[38]
- NEMA DICOM Upper-Level Protocol (ULP) for TCP or DICOMWeb[39] (which includes Web Access to DICOM Objects – WADO) for sharing PACS or RIS information to/from the DHP.
- GS1 Business Messaging Specification (BMS)[40] 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)[41] and Open Authentication (OAUTH)[42] standards for single sign-on functionality

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 an incoming message integration formats, patterns, and data are reconciled prior to message processing continuing within the DHP. Mediation services may include:

- Transformation of messages between data exchange format (e.g., transform FHIR DSTU2 message to FHIR R4)
- Filtering, removing, or appending appropriate message data to inbound 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 in message 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:

[36] Http - FHIR v4.3.0 (hl7.org)
[37] mllp_transport_specification.PDF (hl7.org)
[38] Cross-Enterprise Document Sharing - IHE Wiki
[39] DICOMweb™ (dicomstandard.org)
[40] GS1 XML standards 3.5.1 - GS1 XML | GS1
[41] Final: OpenID Connect Core 1.0 incorporating errata set 1
[42] RFC 6749 - The OAuth 2.0 Authorization Framework (ietf.org)

- 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 may 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 may perform such validation either by sending the transaction to the appropriate service, or by issuing a validation[43] 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 may 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.

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.

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

- HL7 FHIR Capability Statement[44] , Implementation Guide[45] and StructureDefinition[46] resources which describe a FHIR endpoints metadata, allows API operations, etc.
- OpenID Connect Discovery[47] which allows authentication clients to discover the policies (scopes), authorization endpoints and functions of the identity provider infrastructure in the DHP.
- OpenAPI[48] 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[48]. For example, a FHIR REST service within the DHP may 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 solution 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 preferable, however less sophisticated load balancing using DNS is often sufficient (e.g., round-robin). Often a pool of resources is started or stopped based on load on endpoints and active clients. This is to ensure that appropriate quality of service is maintained within the enterprise.

Another part of load balancing is ensuring:

- That a single endpoint (client) does not intensely use the resources of the DHP (service throttling)
- Ensuring the payloads submitted to the DHP via the NHDX are within a certain size limit (i.e., PoS systems are not submitting 5 GB messages to the DHP)
- 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., if the MPI is scaled across two nodes, and one becomes unavailable, the NHDX will forward future requests to the remaining operational node)

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.

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

4.2.3.1.8 Publish and Subscribe

The NHDX implementation should seek to support a publish and subscribe (pub/sub) architecture, which is commonly implemented on enterprise service bus solutions. This functionality is beneficial for the NHDX since it:

- Allows the publisher of information to be isolated from the receiver of the information (i.e., the service bus determines how the message should be routed rather than the caller explicitly calling the recipient). This allows for:
    a. Easier swapping of components (the subscription is merely changed to a new recipient)
    b. Less intrusive change management (services can change network addresses, port numbers, or certificates) independent of any number of callers
- Allows multiple recipients to subscribe to data and triggers
- Allows new recipients to receive data from the NHDX without updating explicit calls or program code to send those messages to a new recipient
- Allows inbound messages and outbound messages to be mediated independently based on the line of business systems' needs
- Allows for more flexibility in supporting a heterogenous environment within the DHP
- Allows for orchestrations of information based on the content of data published to the bus based on events rather than prescriptive workflows

In a pub/sub architecture, messages received from external parties are mediated through an on-ramping procedure (they are validated, transformed, cross referenced, etc.) before being placed onto an internal service bus. The internal service bus matches the information enqueued with registered subscribers which are interested in the published data.

The service bus then performs offramp mediation (validation, transform, cross-referencing, etc.) before despatching the message to the registered subscriber and then on-ramping any response (where the subscription logic is applied again).

Figure 24 provides an overview of how a publish and subscribe pattern works with an enterprise service bus facilitating the reliable delivery of messages between parties.

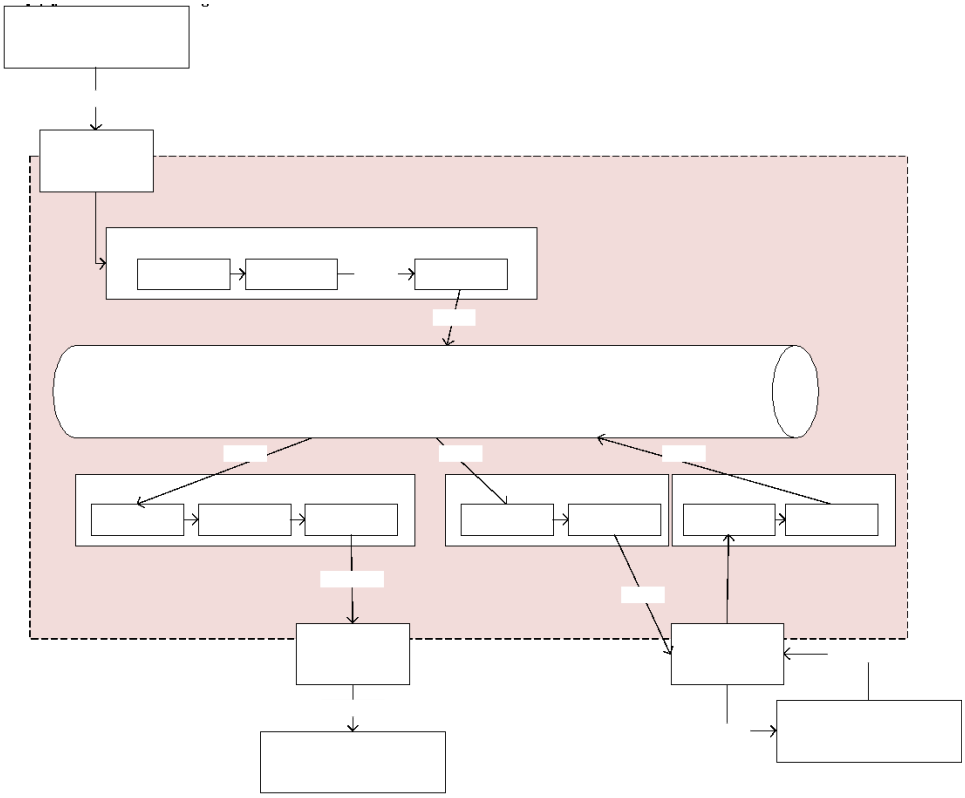

Figure 24- Publish / Subscribe Patterns with ESB

4.2.3.1.9 API Access Control

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

- The API access token in the content of HTTP messages may be used to determine access control rules for the application and user.
- The client certificate submitted with the request (determined by the client certificate the remote node used)

Access control at the NHDX level should only be concerned with the infrastructure access, rather than enforcing privacy or business case specific access control (for example: the NHDX will determine the remote node has access to the NEHR Record Repository query functions, however the NEHR Record Repository should make the determination if the access credential can read data with certain security tags).

4.2.3.2 Terminology Services

Health delivery agencies across the country often use different software and/or different descriptions or terminologies, to describe health information. Records in one system may indicate myocardial infarction where another may indicate heart attack. Without common terminology, the semantic meaning of

records may not be matched. A terminology server also makes it possible to load locally used codes and map these to national/standardised codes, or other local or system level codes.

A terminology server transforms the way in which data is captured, shared, and analysed across health and care, meaning more effective, efficient, and safer decision-making. This makes providing healthcare services, treatment, and cures more efficient and cost-effective.

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[49]:

- Systematized Nomenclature of Medicine Clinical Terms (SNOMED-CT) – Where possible, use of the Global Patient Set (GPS)[50] is encouraged.
- International Classification of Disease (ICD) Release 10[51]
- Logical Observation Identifiers Names and Codes (LOINC) version 2.67 or later[52]

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)
- 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").

[49] National Digital Health Guidelines and Standards [2] Section 7.6
[50] SNOMED - Global Patient Set
[51] ICD-10 Version:2010 (who.int)
[52] Download LOINC – LOINC

The concept of a record locator mimics the functionality of a *Document Registry* in the IHE XDS profile[53] 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)
- A digital signature or checksum of the original data to allow for verification

Implementation of a record locator service may not be necessary in early implementations of the blueprint where a single NEHR Repository services as the sole repository of information – however it becomes more useful in future iterations as multiple repository services are implemented.

4.2.3.4 Order Fulfilment

The order fulfilment services in the shared infrastructure components are intended to provide correlation services between transactions order and fulfilment workflows. The blueprint does not explicitly prescribe the way this order correlation occurs, however a general pattern of this type of information is illustrated in Figure 25.

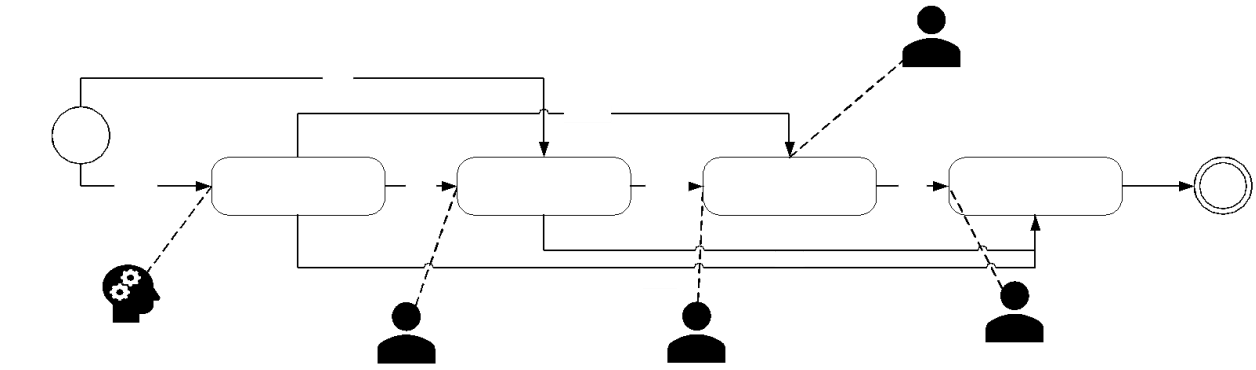

Figure 25- General Order Flow

The order correlation service is meant to link together (or ensure/maintain appropriate links) throughout the data flow of order and fulfilment.

A decision support system may recommend (PROPOSE) a course of action occur. This can be a medication proposal, an imaging proposal, a laboratory proposal, a recommendation to immunise a patient, or any other clinical action.

[53] IHE ITI TF Vol1 Cross Enterprise Document Sharing

A human user may then turn this proposal into a direct request (ORDER), or a human user may directly create a request. This can be a prescription (in the case of a medication order), an imaging requisition, or lab requisition.

At a future state, the DHP can support points of service querying for outstanding requests and, based on their own capacity and availability may issue an intent to fulfil the order (PROMISE). Storage of intents to fulfil orders should be linked with the original request and can be used to prevent multiple fulfilment scenarios in a distributed system. This type of information may be submitted as a medical formulary notification, a despatch, or an appointment for sample collection or the procedure.

Once the intended action has occurred (FULFILL) a preliminary and/or final output is recorded in the DHP. This output may be a diagnostic report, radiology, or pathology report, an immunisation event or a medication dispense.

Whatever the nature of the output, it is important that the information received into the DHP is correlated and linked. Such linkages are beneficial as they allow for:

- Health System Response Time – By linking together records through a proposal, request, intent, and fulfilment process, it is possible to determine the length of time a single action took i.e., “wait time”.
- Completeness – By linking together records through the order/fulfilment flow it is possible to see incomplete, or unactioned requests.

4.2.3.5 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.

Additionally, attempting to coordinate a clinical flow across multiple repositories may 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, transform, cross reference data, and/or notify secondary repositories.

4.2.3.6 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 may 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 health administration domain is described in the business architecture in Healthcare Administration, on page 85. The conceptual components of the health administration domain are illustrated in Figure 26.

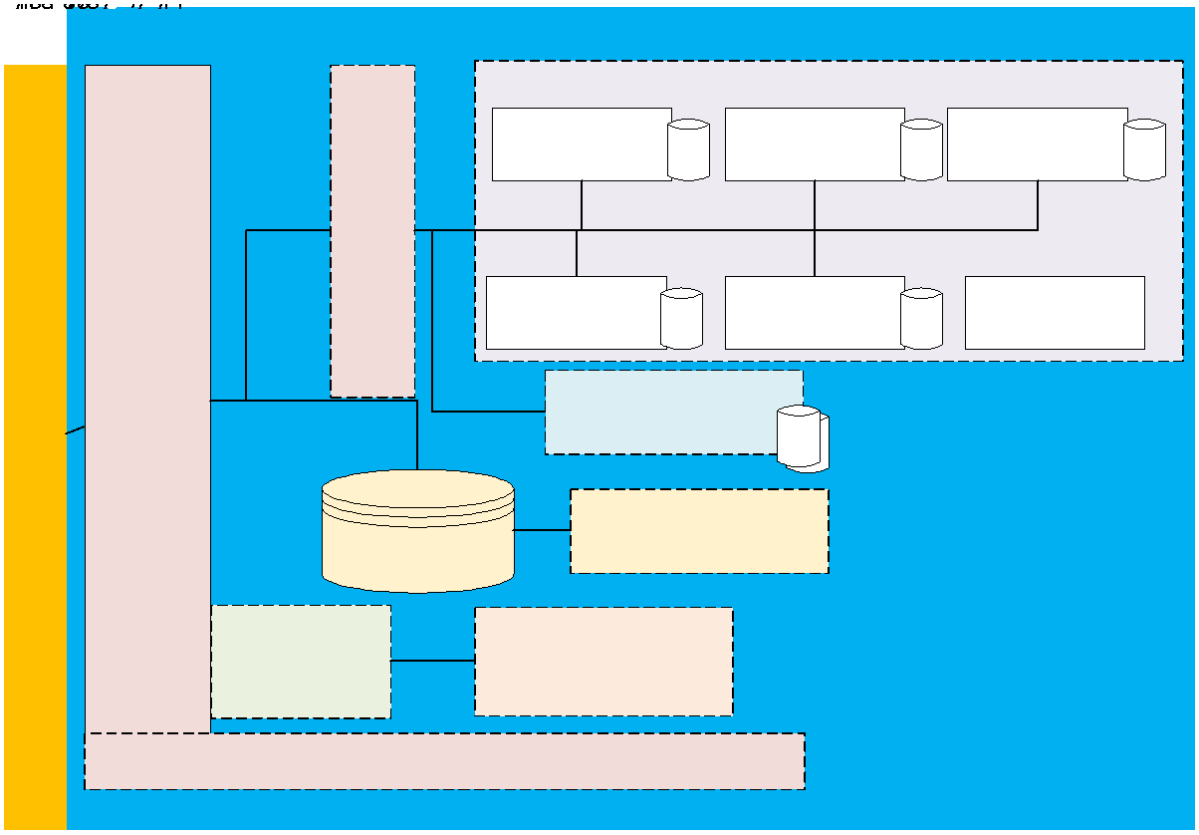

Figure 26- Health Administration Conceptual Components

4.2.4.1 Client Registry / Master Patient Index

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 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 master patient index within a healthcare enterprise is well defined[54,55] , at a high level the master patient index in Sri Lanka is expected to:

- 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)

[54] IHE.ITI.PMIR\1:49 Patient Master Identity Registry (PMIR) Profile - FHIR v4.0.1
[55] Client Registry (CR) - OpenHIE Architecture Specification (ohie.org)

- 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[56] and be capable of cross-referencing the following identifiers to an enterprise unique identifier:

- Citizen Identification Number
- National Identity Card Number (NIC)
- Sri Lanka Identification Number (SLIN)
- Personal Health Number (PHN)
- Passport Number (for foreigners)

Because the MPI in a national or provincial realisation of the blueprint may contain demographics for all citizens, for privacy reasons it is proposed that demographics-based queries (discovery of patients using their demographics) be restricted in one of the following manners:

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

4.2.4.2 Healthcare Provider (Worker and Organisation) Registry

The distribution of health records across organisations and services necessitates the consistent identification of those persons and organisations which are responsible for the delivery of care services. This is the primary role of the healthcare 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.

The primary responsibility of a provider registry is well defined[57,58] and can generally be summarised as:

- Accepting official registrations and updates from official licensing bureaus, national professional associations, colleges, commercial registries, human resources information management solutions for providers.
- Providing a linkage between the official licensing / qualifications of a provider to deliver a specific type of care and classification of organisations/persons based on their speciality (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.
- Discovery of health providers (persons or organisations) based on their registration details (such as address, telephone, name, or services)

[56] National Digital Health Guidelines and Standards [2] Section 7.2
[57] IHE Health Provider Directory Supplement
[58] OpenHIE Health Worker Registry (HWR) - OpenHIE Architecture Specification (ohie.org)

The provider registry in the DHP should implement the minimum dataset[59] for providers, and should be capable of cross referencing the following identifiers with an enterprise unique identifier with:

- Professional Registration Number and Issuer (college, association, or other)
- National Identification Number (NIC)
- Sri Lanka Identification Number (SLIN)
- Legal Registration or Incorporation Number (for organisations)
- Other individual provider identification numbers, for example:
    a. Private Sector Hospital Registration
    b. Passport Number (for foreign or visiting providers)
    c. Tax Identification Numbers (for organisations)

4.2.4.2.1 Human Resources Management Information Systems

Human Resource Management Information System (HRMIS) solutions in Sri Lanka have been adopted by various units and departments[60], and can provide the basis for populating an independent health provider registry. The use of the HRMIS as the provider registry is discouraged since:

- The provider registry must maintain a list of all providers in the DHP including those registered/hired at a provincial level or those working or hired in a private sector institution
- The HRMIS solutions are typically focused on HR business processes of active staff under the employ of the operator of the HRMIS
- The provider registry should include organisational providers' registration details and offered services.

However, human resourcing and allocation of personnel between organisations, and facilities is still a vital component of the broader enterprise and is therefore called out as a component of the proposed DHP solution.

4.2.4.3 Healthcare Facility Registry

The health facility registry is responsible for the maintenance of a country-wide manifest of public and private facilities which for which data may be registered in the DHP. The role of a facility registry is well defined[61] , and can be summarised as:

- Collect, store, and disseminate an authoritative master facility list (MFL) of clinics, hospitals, specialist providers, and other locations where health services are provided
- 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 of facility information to allow for consistent identification of facilities between systems
- Provide query capabilities allowing other digital health services to locate service delivery locations which provide specific services, located in a particular geographic area, or which have certain capabilities and capacity.

[59] National Digital Health Guidelines and Standards [2] Section 7.4
[60] 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
[61] OpenHIE Facility Registry Implementation Guide - Google Docs

The facility registry in the DHP should implement the minimum dataset specified for Sri Lanka[62] and should provide functionality for cross referencing local identifier for facilities (obtained from source registration systems for facilities) with a unique enterprise identifier.

4.2.4.3.1 Existing Systems

MOH Sri Lanka currently maintains several systems which use facility information including staffing allocation and transfer request management, HRMIS, the national health facility survey management system, and implementations of DHIS2. These systems may serve as the basis for establishing a master facility list.

4.2.4.3.2 Interlinked Registries & Care Service Discovery

It is possible to implement the functionality of a healthcare provider registry and facility registry as several, independent interlinked registries for organisations, facilities, and health workers. Such implementations should expose functionality using appropriate care service discovery standards[63,64] using an interlinked registry.

4.2.4.4 Medication / Drug Registry

The registration of a central drug registry is of high importance for providing a definitive list of qualified medications which may be referenced within the digital health blueprint.

A medications and drug registry will be used to track the substances (supplements, vaccines, therapeutics, or other) 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 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

A medication and drug registry solution should be capable of tracking:

- Registered drug product name and brand or trade name
- Unique identification of the product (manufacturer identification, GTIN, and other identifiers)
- Drug classification code using WHO ATC[65], SNOMED CT[66], CVX[67], or other appropriate nomenclature
- Manufacturer/Supplier demographics (name and contact information)
- Packaging/presentation of product (10 dose vials, pre-packaged syringe, pills, oral drops or other)
- Dosing quantity and recommended dosing frequency

[62] National Digital Health Guidelines and Standards [2] Section 7.3
[63] Care Service Discovery (CSD) Supplement
[64] Mobile Care Services Discovery (mCSD) - IHE Wiki
[65] Anatomical Therapeutic Chemical (ATC) Classification (who.int)
[66] Drug or medicament (snomedbrowser.com)
[67] IIS | Code Sets | CVX | Vaccines | CDC

- Current regulatory status and alerts for products (awaiting approval, active, withdrawn, recalled, etc.)

The implementation of the medications and drug repository may implement appropriate HL7 FHIR[68] resources as well as appropriate logistics support messages such as GS1 BMS Product Recall[69] and Item Data[70] transactions.

4.2.4.5 Equipment & Supplies Registry

The ordering and reporting of medical devices and 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.

Additionally, providing of medical devices to patients such as insulin pumps, pacemakers, or prosthetics should have linkages back to a registration for those devices.

The primary functions of the equipment registry are:

- Collect, store, disseminate registration information of new devices 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, medical device installation procedures and stock orders/despatches/arrivals to registered devices.
- Provide a master list of device regulatory information including status (pending, active, withdrawal, etc.), manufacturers, and suppliers.

Given the similarity of this registry to the drug and medication registry, it is likely an implementation may use a single solution for both business goals.

The implementation of the equipment and supplies repository may implement appropriate HL7 FHIR[71] resources as well as appropriate logistics support messages such as GS1 BMS Product Recall[69] and Item Data[70] transactions.

4.2.5 Health Delivery

The health delivery business domain is described in section 3.3.5.4 on page 86. The primary purpose of the DHP services contained within the health delivery business domain service the needs of managing information and processes which facilitate the delivery of care. The components within this domain are illustrated in Figure 27.

The proposed solution accommodates the disclosure and contribution to a shared patient summary (the National Electronic Health Record) which already has a defined patient summary dataset[72], via a dedicated clinical data repository (the NEHR Repository). However, to accommodate growth into future disease vectors, to support workflows beyond patient summaries, additional repositories may need to be

[68] Medication - FHIR v4.3.0 (hl7.org)
[69] Product Recall | GS1
[70] Item Data Notification | GS1
[71] Device - FHIR v4.3.0 (hl7.org)
[72] National Digital Health Guidelines and Standards [2] Section 7.7

implemented to isolate data, support specific clinical data use cases, or special types of data (such as non-FHIR data including DICOM, GS1, HL7 CDA, etc.).

Additionally, the solution separates the information repositories from components which store the definition of rules, and execution of those rules. This separation of concerns allows clinical decision support definitions to be disseminated between any solution within the DHP or executed by the DHP (as a CDSS-as-a-service model).

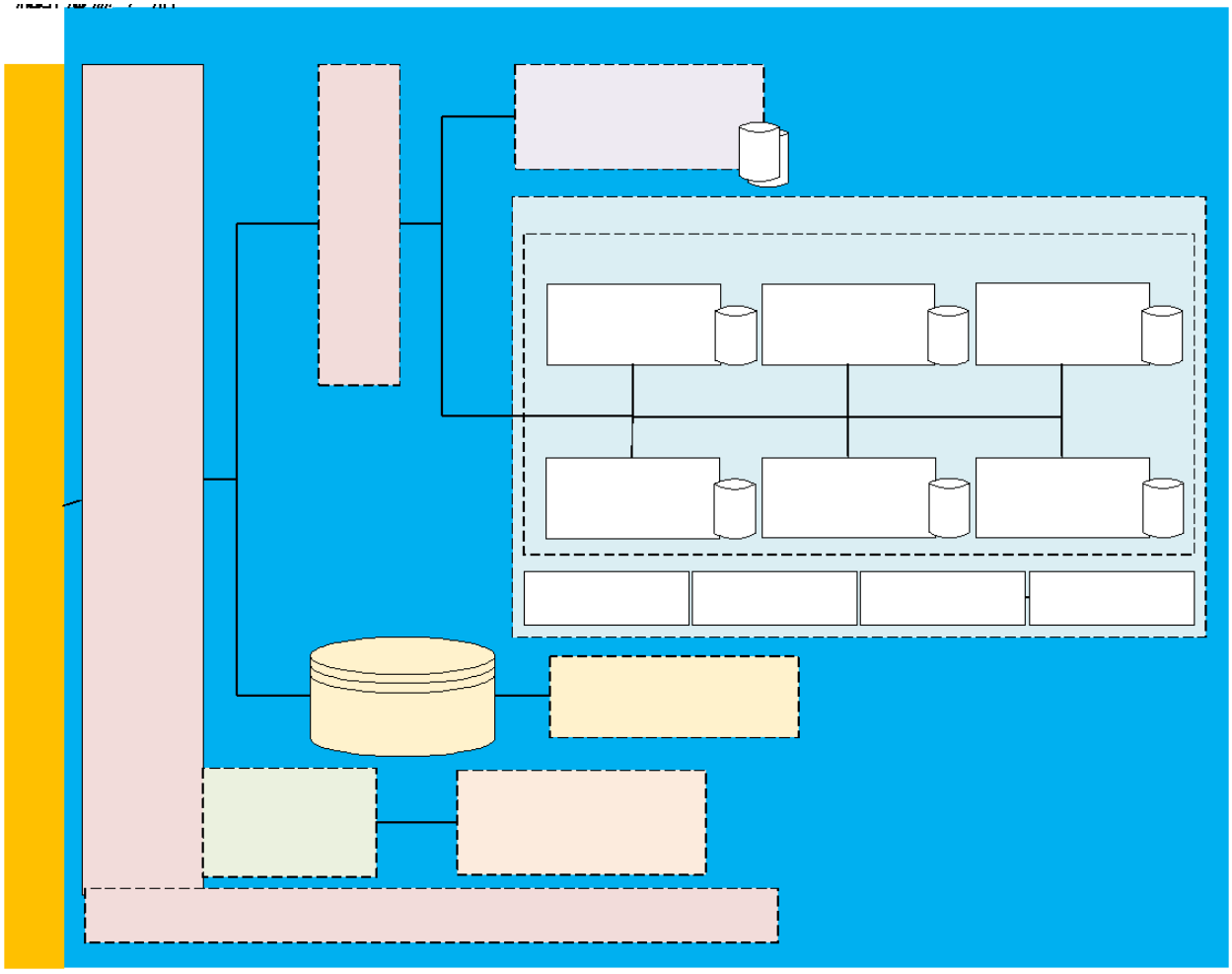

Figure 27- Health Delivery Domain Conceptual Components

4.2.5.1 National Electronic Health Record (NEHR) Repository

The minimum dataset for a standing, shared patient summary was defined in the NDGS[73]. The goal of the NEHR Record Repository is to provide the necessary storage and retrieval capabilities for this data. The primary responsibility of the NEHR is to be set out in a NEHR Record Repository solution view, however its conceptual purpose in the context of the DHP is to:

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

- 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 137. 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 radiological studies within Sri Lanka. Due to the infrequent requirement to access, and the size of the original modality images, it is not desirable nor feasible to replicate these data files between all points of service.

The DHP proposes alignment with the pattern defined in the IHE Cross Enterprise Document Sharing for Imaging (XDS-I)[74] profile. In this pattern, only the 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.) may query for and retrieve manifests and radiology reports.

If the user of the images (the point of service consuming the manifest) wishes to retrieve the full image (which may be gigabytes of data) they should do so directly from the RIS using a mechanism similar to that defined in 4.2.2.5.1 Transfer of Large Data Objects on page 96.

Figure 28 provides an illustration of the IHE XDS-I profile with a mapping to services/components within the DHP.

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

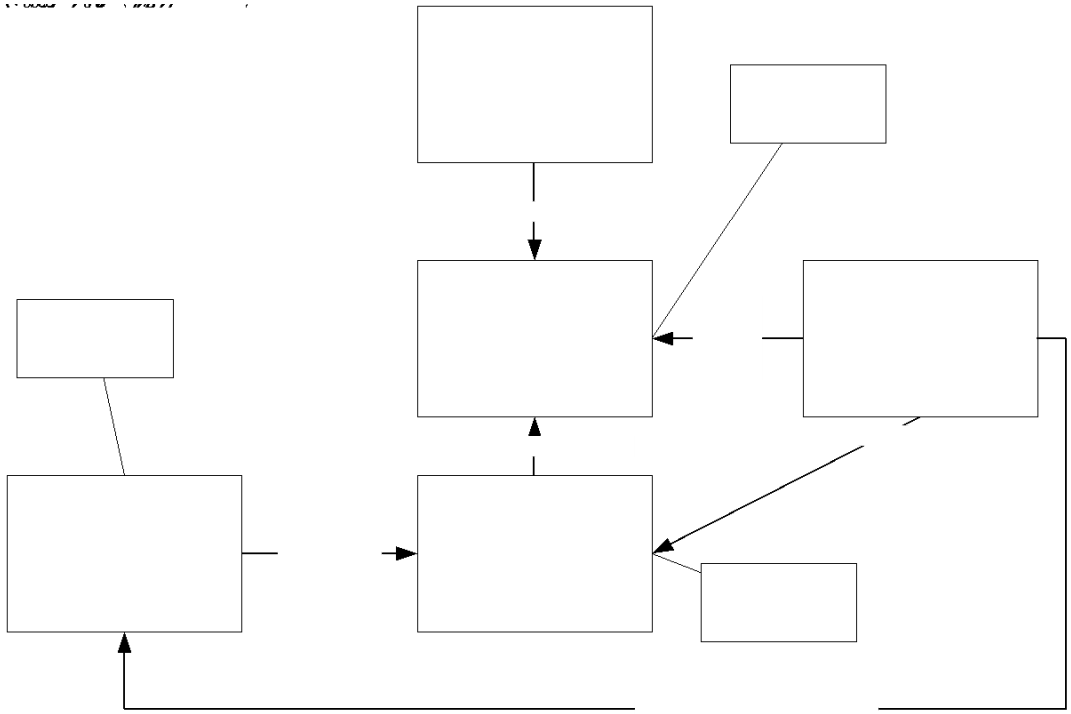

Figure 28- XDS-I Image Exchange in DHP

4.2.5.3 Disease or Domain 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 domains, introducing standards to these technologies, and using them as the repository of information fosters reuse (and reduces data migration)
- Specialised validation logic for a particular disease or domain of health care can be separated in smaller solutions instead of a large monolithic solution
- Different standards can be adopted based on their applicability to the problem domain and maturity

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[75] architecture and allows for a single table of contents to reference multiple repositories which are more well suited for their domain of expertise.

[75] IHE ITI TF XDS.b Vol1

4.2.5.3.1 Isolating Resources Based on Maturity

HL7 FHIR within large-scale integrations presents challenges as the standard can structurally change from time to time between releases, and new releases may contain breaking changes on resources which are not fully mature[76]. For example, AdverseEvent (FMM-0) could contain breaking changes between versions. Additionally, specific functions such as an immunisation registry would require implementing resources of varying maturity such as: Immunization (FMM-3), ImmunizationRecommendation (FMM-1) and ImmunizationEvaluation (FMM-0) which all may introduce breaking changes between releases.

At the time of writing approximately 9% of FHIR resources are "normative" and the remaining 91% are deemed "trial use"[77].

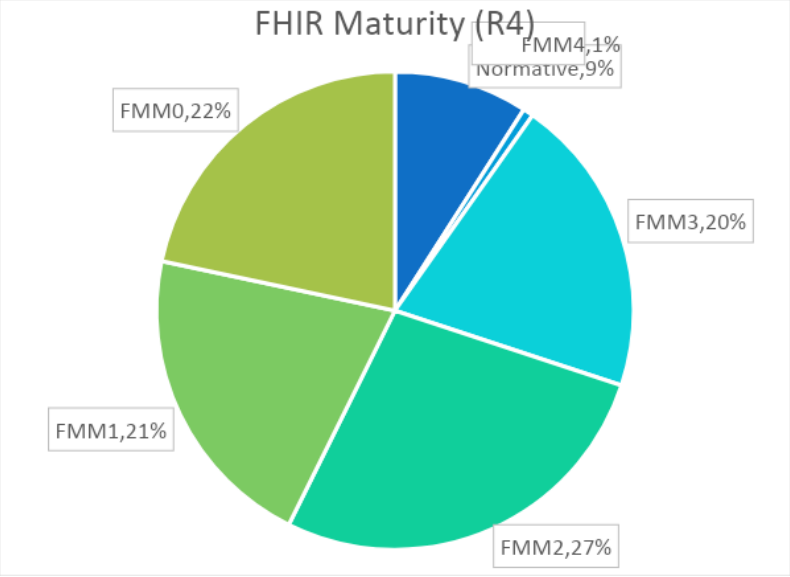

Figure 29- Maturity of FHIR Resources (as of R4)

Because of this, migrating a single monolithic repository of data to a new version of FHIR may break functionality for consumers and producers of that information, which is not desired in a widespread enterprise implementation.

HL7 FHIR is continuously evolving, and it is important that these changes be isolated and do not impact the stability of the various business domains being serviced. The infostructure must be protected from the practicalities of using multiple revision levels various states of maturity. It is important to understand and potentially isolate specific domains where the resources have not reached a sufficient level of maturity. For example, a new domain point of service application using FHIR R5 must not corrupt the entirety of the NEHR data which may have previously used FHIR R4 at the point of service.

The DHP seeks to solve this problem by proposing that only resources needed for the NEHR, or resources which are of FMM3 or higher (representing only 30% of available resources) are adopted within the NEHR repository, and resources which are of a lower maturity be adopted on a use-case need in domain

[76] FHIR Maturity Model - FHIR - Confluence (hl7.org)
[77] Resourcelist - FHIR v4.3.0 (hl7.org)

or disease specific repositories, where changes and breakages to resources will only yield that domain unavailable or un-readable by consumers and producers of data.

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 a physician (example: discharge summary from a hospital)
- 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[78]:

- *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 such as a PDF, PNG, TIF, etc.
- *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 may be un-structured.
- *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[79] 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)[80] and Mobile Health Document Sharing (MHDS)[81] profiles provide a useful pattern for storing this information within the DHP. Figure 30 shows how the MHDS and MHD profiles from IHE logically map onto business services within the DHP.

[78] HL7 CDA | Lyniate
[79] Documents - FHIR v4.3.0 (hl7.org)
[80] IHE.ITI.MHD\MHD Home - FHIR v4.0.1
[81] IHE.ITI.MHDS\1:50. MHDS Volume 1 - FHIR v4.0.1

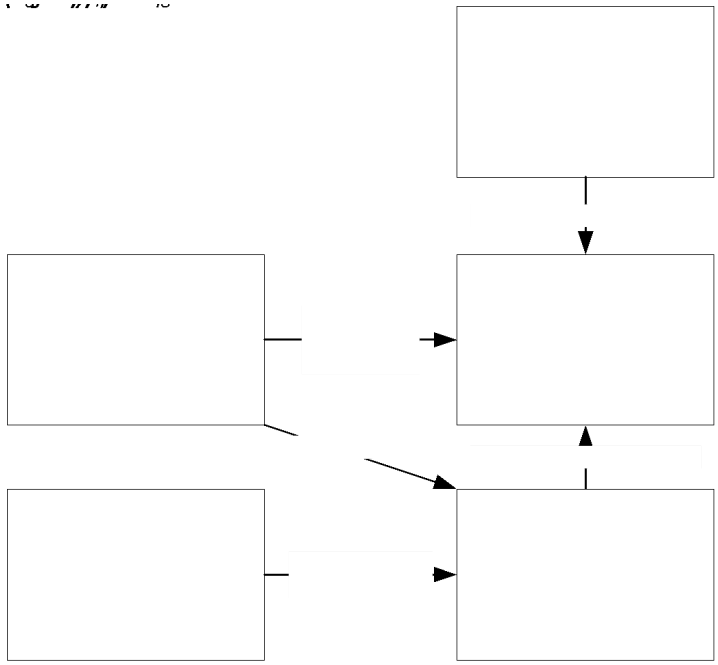

Figure 30- MHD and MHDS in the DHP

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.
- 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)[82] represent a more widely adopted and mature series of interchanges for logistics.

The NHDX does not specify whether the inventory and logistics data will be a central repository model (where a logistics management information system receives and manages all inventory data) or a peer model (where each point of service exposes BMS endpoints for requesting logistics reports and orders) as is traditionally used in supply chains.

[82] GS1 set of XML standards | GS1

4.2.5.6 Care Guidelines Repository

Computable Care Guidelines (CCG)[83] are increasingly gaining traction as a method of implementing best practices within the health enterprise. CCGs allow the specification of rules and computable logic for care pathways and provide mechanisms for measuring the adherence to those guidelines.

The DHP proposes the care guidelines repository for the storage of artifacts which define common computable care guidelines within the Sri Lankan health enterprise. This will foster the implementation of CCGs such as WHO's SMART Guidelines[84] by providing services for the storage and dissemination of L2 (operational descriptions) and L3 (machine readable) artifacts within the Sri Lankan enterprise.

The contents of this repository will include:

- Implementation guides which contain the overall narrative and technical descriptions of the standardised guidelines, adapted for Sri Lanka
- Definitions and conformance statements for the structure of data which needs to be captured from points of service
- Libraries[85] 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 may be able 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[86] architecture.

4.2.6 Secondary Use

The secondary use business domain is defined in section 3.3.5.6, on page 88. The conceptual services which compose the secondary use domain, and sample use cases of secondary use data are illustrated in Figure 31.

[83] Computable Care Guidelines - IHE Wiki
[84] SMART Guidelines (who.int)
[85] Library - FHIR v4.3.0 (hl7.org)
[86] CDS Hooks (cds-hooks.org)

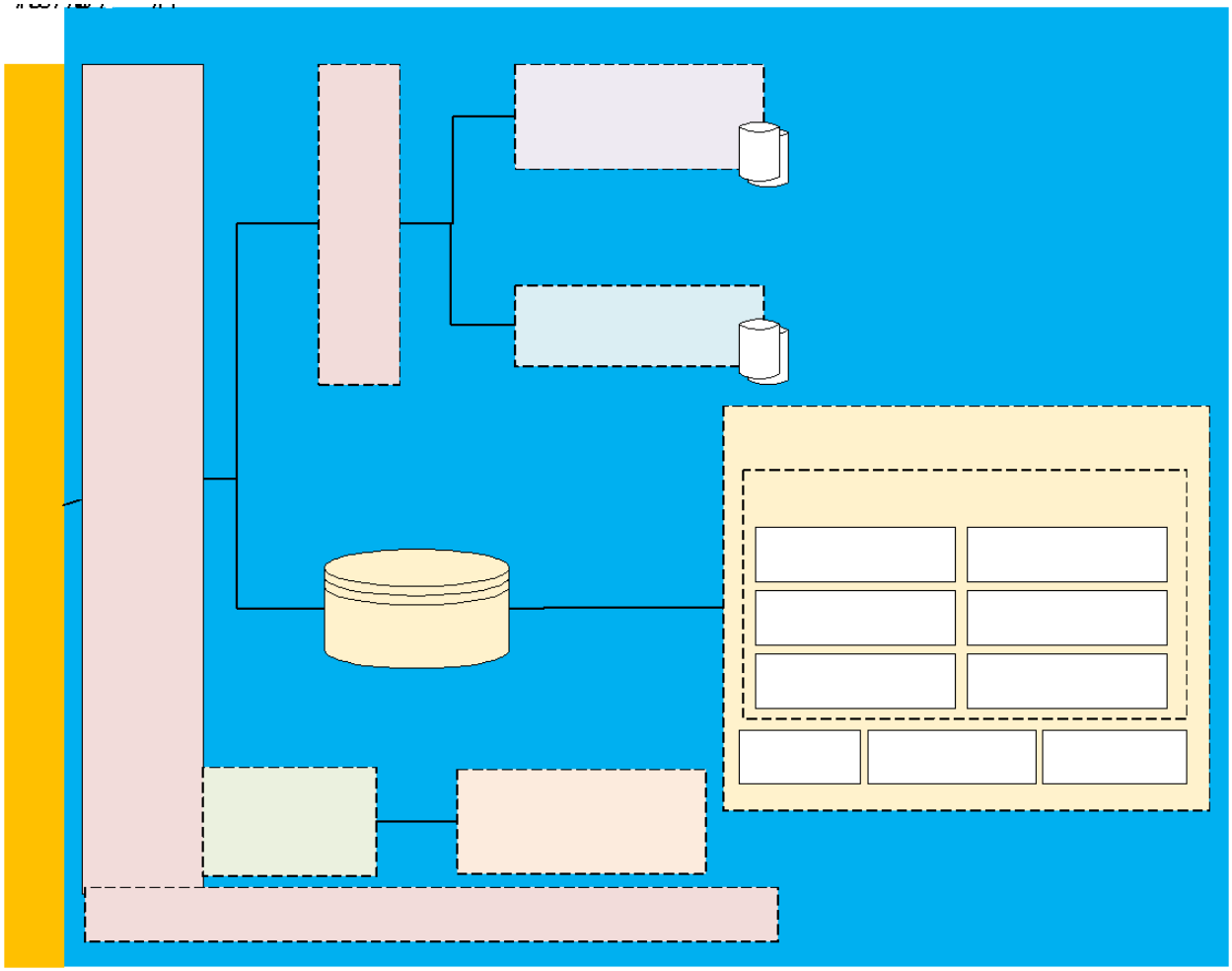

Figure 31- Secondary Use Domain Conceptual Architecture

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 DHIS2. 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[87] and health system status questionnaire responses[88] submitted to the DHIW service via the NHDX
- Population of data directly from NHDX triggers / subscriptions as data flows through the enterprise
- Receipt of aggregate data exchange (ADX) measurements from existing databases.
- Disclosure of indicator measure values via APIs (ADX, or HL7 FHIR MeasureReports[87]) which can be used by authorised third-party solutions for data-driven analysis within their own solution.

[87] MeasureReport - FHIR v4.3.0 (hl7.org)
[88] QuestionnaireResponse - FHIR v4.3.0 (hl7.org)

Fostering a culture of information sharing with researchers and institutions and providing the basis for Open Government[89]

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 5.2.5, on page 140.

The DHIW may be a singular implementation or a heterogenous implementation using several different strategies for secondary use data storage spread across different systems comprising the DHIW including:

- Traditional RDBMS (Relational Database Management System) warehouse schema with defined data marts using a standardised practice such as Data vault[90] 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

The future state of the blueprint is an electronic dissemination of KPI definitions and questionnaires which can be used by points of services and registry/repository applications for the purpose of calculating values for each indicator defined by provincial or central governments.

While this is a lofty goal, the reality is that the inclusion of the mechanisms for distribution, completion, and conveyance of results of these structures may not be widely available for some time. To bridge this gap, the blueprint proposes the leveraging of extract, transform and load[91].

ETL jobs are defined by data analyst teams and written in software which supports the bulk loading and transformation of data (such as Talend Open Source) 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.

4.2.6.1.2 KPI Definitions Repository

The blueprint proposes the implementation of a repository which can be used to allow the central and provincial ministries of health to define their own indicators for which they would like points of service, 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)[92] or Structured Query Language (SQL)[93]
- As FHIR definitions such as:

[89] Open Government - Canada.ca
[90] Data vault modeling - Wikipedia
[91] Extract, transform, load - Wikipedia
[92] Clinical Quality Language (CQL) (hl7.org)
[93] sql1999.pdf (pdx.edu)

a. Measure[94] - for data which can be computed directly from FHIR resources
b. Questionnaires[95] - 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

Included in secondary use of data is the process for removing individually identifiable information from healthcare data. The de-identification service within the secondary use domain will provide services for the appropriate de-identification of data based on requirements.

Modern techniques are available to protect patient privacy while still providing valuable data for secondary use and include de-identification, pseudonymisation, and re-linking considerations. The domain solution guide will describe various techniques and risks presented to digital health solution implementers as a guide for designing and implementing de-identification systems.

ISO/TS Standard 25237[96] 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.

De-identification is used to reduce privacy risks in a wide variety of situations:

- Complete de-identification can be used for materials that will be made widely public but will still convey enough detail to be useful for medical and educational purposes.
- Public health uses de-identified databases to track and understand diseases and outbreaks.
- Clinical trials use de-identification both to protect privacy and to avoid subconscious bias by removing other information such as whether the patient received a placebo or an experimental drug.
- Less complete de-identification can be used in clinical reviews where the reviewers are kept ignorant of the treating physician, hospital, patient, etc. both to reduce privacy risks and to remove subconscious biases, however with some effort the patient identity can be discovered.

Public health and clinical trials will likely have a requirement to be able to contact a person based on their re-identified records. This will also help to determine the methods used to initially de-identify the

[94] Measure - FHIR v4.3.0 (hl7.org)
[95] Questionnaire - FHIR v4.3.0 (hl7.org)
[96] https://www.iso.org/standard/63553.html

records. The information flow and process for de-identification is described in further detail in section 5.2.7.3.1 on page 147.

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 DHP Building Blocks).

The shared services related to privacy and security are illustrated in the context of the broader digital health platform in Figure 32.

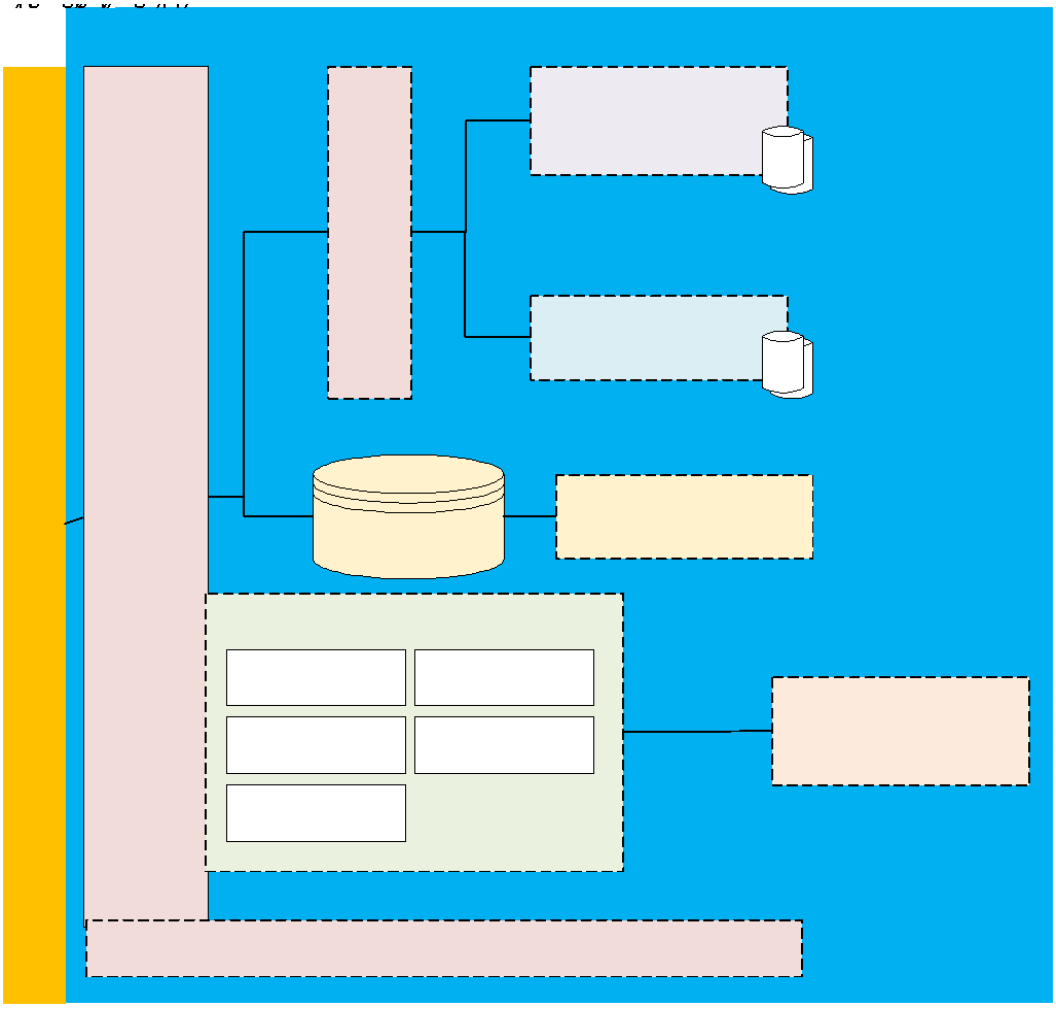

Figure 32- Security & Privacy Domain Conceptual Architecture

4.2.7.1 Time Keeping / Consistent Time

Consistent time keeping may seem like a trivial concern, however 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)[97] and the considerations for an enterprise timekeeper is described in IHE Technical Framework[98].

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[99]
- A key distribution service (KDS) which allows services to obtain public keys for validation of signed data following the JSON Web Key[100] specification. The key distribution service should be publicly available and should use the JSON Web Key Set[101] 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[102] 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[103])

The chain of trust for the DHP can be based and delegated based on provincial and central areas of concern as illustrated in Figure 33.

[97] RFC 1305 - Network Time Protocol (Version 3) Specification, Implementation and Analysis (ietf.org)
[98] IHE ITI TF Vol1 - Consistent Time
[99] RFC 3447 - Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 (ietf.org)
[100] RFC 7517 - JSON Web Key (JWK) (ietf.org)
[101] JSON Web Key Sets (auth0.com)
[102] IHE ITI TF Vol2 – Authenticate Node
[103] SMART Health Cards Framework

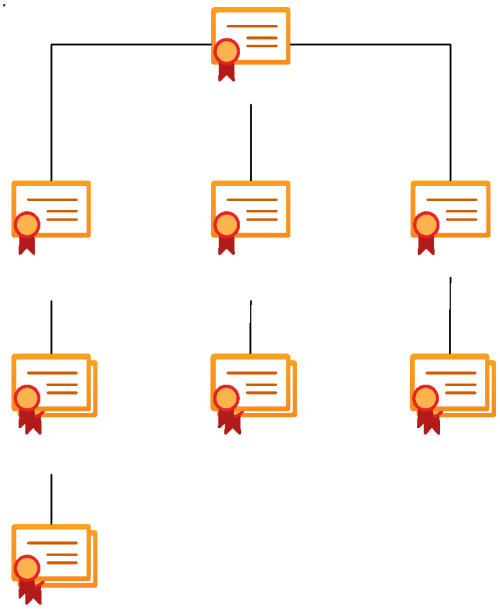

Figure 33- Certificate Chain of Trust

This pattern:

- Allows for delegation of access to the DHP for nodes to departments
- Allows for revocation of certificates at a device, institution, or central level
- Allows for identification of a node or digital signatory with the chain of issuance/trust (i.e., HHIMS as General Hospital, Issued by General Hospital, Issued by Uva Province, Issued by DDG MSI, Issued by MOH)

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[104]. The blueprint strongly proposes the DHP provide one or more centralised audit record repositories 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. A well-supported audit repository within the DHP allows administrators to:

- Produce privacy accounting and disclosure reports which indicate to whom and when a disclosure was given
- 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
- Prove that a user inappropriately accessed a VIP patient

[104] National Digital Health Guidelines and Standards [2] 6.3.3

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?

Individual participants within the DHP should strive to keep localised audit trails within their own system software and should forward audits to a centralised repository of audits as well.

It is typically best practice (as documented in IHE Record Audit Event[105]) that mirrored audits are provided to the system. This can be used to detect irregularities in access logs (i.e., the sender recorded an event, but the recipient never recorded the matching event, so the message may have been redirected).

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[106] 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)[107]
- NEMA DICOM Audits[108]
- HL7 FHIR AuditEvent[109] resources (preferably using a standardised profile such as the RESTful ATNA profile from IHE[110])

The logical information model of the structure and contents of audits is discussed in further detail in section 5.2.5 on page 140.

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. To facilitate consistent auditing, access control, and business rule execution between each of these services is it important that the identity of the user, their granted scopes, roles, application, and devices are conveyed throughout the entirety of the DHP as requests are routed from service to service.

The blueprint proposes that a bearer token strategy be used to facilitate the transmission of authentication context between instances. The bearer token will be generated and digitally signed (to prevent tampering) from a centralised identity provider. The blueprint recommends using OpenID

[105] IHE ITI TF Record Audit Event - Vol2
[106] IHE ITI TF Audit Trail and Node Authentication - Vol1
[107] RFC 3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications
[108] A.5 Audit Trail Message Format Profile (nema.org)
[109] AuditEvent - FHIR v4.3.0 (hl7.org)
[110] IHE_ITI_Suppl_RESTful-ATNA

Connect[111] which is based on OAUTH[112]. This implementation is compatible with the SMART on FHIR[113] pattern of integration as well as IHE Internet User Authorization (IUA)[114].

The implementation of the identity provider may manifest as a single identity solution operated by the ministry of health or may be a federated solution where multiple identity providers are trusted by the DHP. The blueprint proposes that, regardless of the manifestation of the IdP, the access and identity tokens should follow a consistent format and assertion pattern such as the JSON Web Token (JWT)[115] format.

4.2.7.4.1 Application Authentication

Many of the software services within the DHP will need to authenticate EMRs and remote systems in a consistent manner. In a typical application authentication scheme, a client identification and API key are issued to valid clients, this information can be used to authenticate the remote system without the need of using certificate-based authentication schemes.

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.

The client credentials grant flow specified by OAUTH is illustrated in Figure 34.

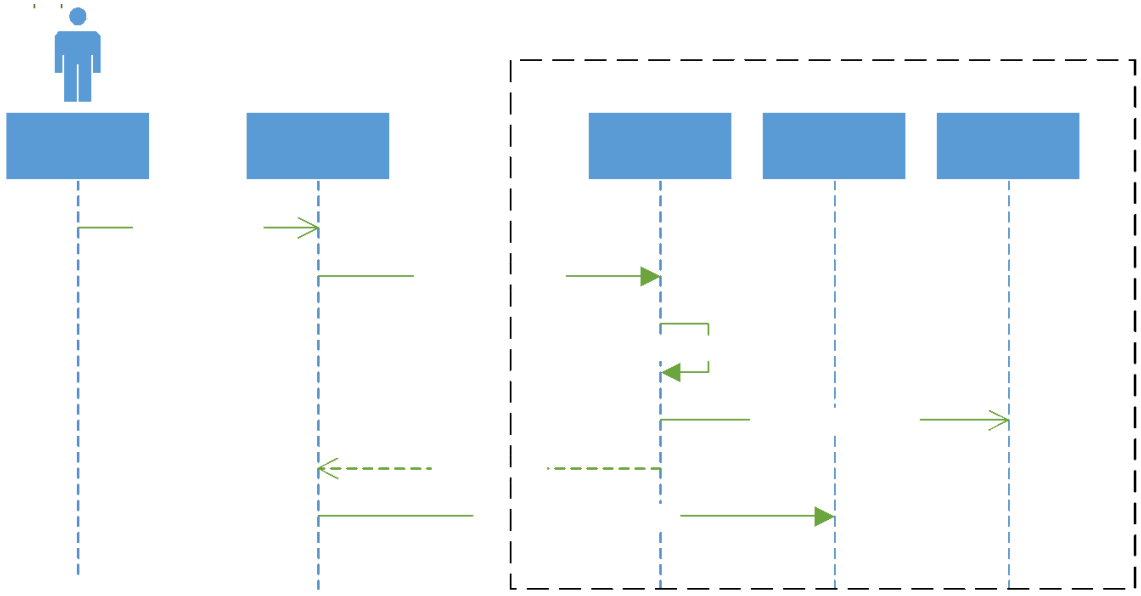

Figure 34- Client Credentials Flow

[111] Specifications | OpenID
[112] Map of OAuth 2.0 Specs - OAuth 2.0 Simplified
[113] HL7.FHIR.UV.SMART-APP-LAUNCH\Overview - FHIR v4.0.1
[114] IUA (ihe.net)
[115] RFC 7519: JSON Web Token (JWT) (rfc-editor.org)

In this flow, an application will send a client identifier (example: openmrs-tb-site3) and a client secret (a random API key generated when the application is validated). The identity provider responds with:

- A digitally signed identity token which provides assertions (claims) about the holder of the validated identity.
- A digitally signed access token, which provides information about the access for the application as the token is sent around the DHP.
- A digitally signed refresh token which can be used to extend the session rather than triggering a new re-authentication

4.2.7.4.2 User Authentication

The identity provider should support the authorisation code flow, illustrated in Figure 35. This flow is the standard flow which users should be familiar with as it is the same technology used for Google, Microsoft, Apple, and other authentication methods on the internet.

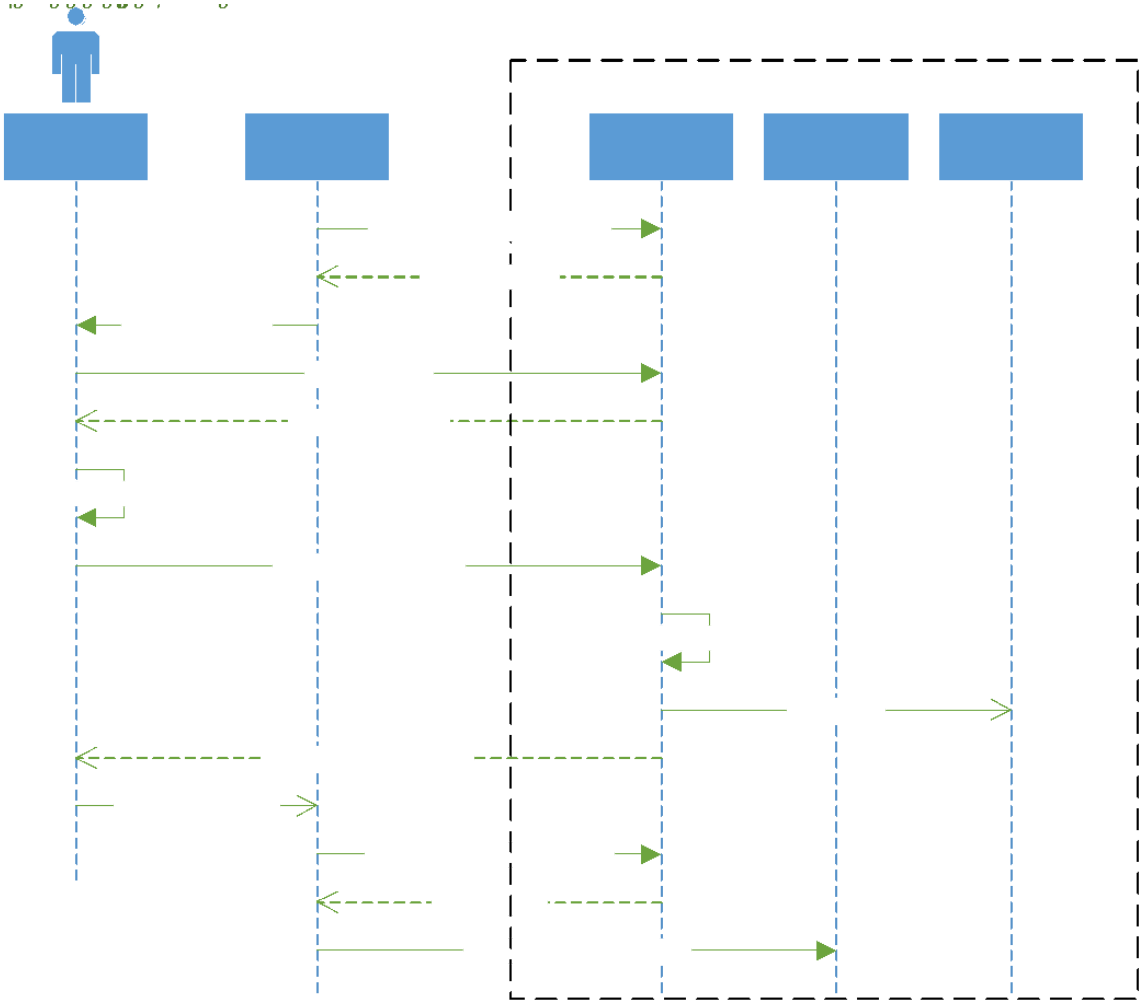

Figure 35- Authorization Code Flow

In this model, the user's central DHP password is never disclosed to the point of service, rather the point of service is given a claim token which can be used to obtain a digitally signed token response. The response from the identity provider should contain:

- An access_token which is a digitally signed token used for accessing DHP resources. This access token is placed in the header of all requests to the NHDX which should maintain this information when calling back-end services
- An identity_token which is a signed JSON Web Token (JWT)[116] containing information about the identity
- A refresh_token which can be used by the point of service to extend the bearer token beyond its initial expiration

4.3 Proposed Governance of DHP Service Definitions

As described in section 2.3.1 on page 30, this blueprint document sets forth the enterprise view of the digital health ecosystem in Sri Lanka. This enterprise view defines the building blocks which serve as the basis for developing solution and subsequent technical views. These views should indicate more specific information flows, data requirements, and standards for the individual business function(s) which are being defined or profiled.

This section proposes a framework for the development of these further detailed views of the health enterprise within Sri Lanka.

Governance is an integral element of and key requirement for the establishment of a national digital health platform and National Electronic Health Record (NEHR). It is recommended that the collaborative development process include public and private health organisations, national and local jurisdictions, academics, standards-related organisations, healthcare professionals and technology providers that will build, operate, and use the digital health platform.

The initial set of business domains and services has been identified and proposed throughout sections 3.3 and 4.2. It is inevitable that, as the DHP evolves, further specification as well as new business domains and services will be required over time. This section proposes an initial governance process for organising, developing and reviewing future solutions and services.

Note: It is recommended that a detailed governance process be developed and documented as part of the standard operating procedures of managing the digital health platform implementation program.

1. A need for a new Business Domain is identified by clinical or administrative users
2. The details and scope of the Domain are established
3. The scope is reviewed by an *Architectural Review Board*[117] (ArB) that is responsible for maintaining the architecture and the Blueprint
4. ArB conducts an alignment check with stakeholders
5. If proceeding, the domain Technical Working Group (TWG) committee is formed (e.g., Genomics, Terminology, etc.)
6. The Domain TWG conducts the analysis of services which need to be integrated into the blueprint.

[116] JSON Web Token Introduction - jwt.io
[117] https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap41.html

7. The Domain TWG will continue with development of solution views documentation (detailing the business needs, appropriate standards, and transactions of the domain)
8. The Domain TWG presents draft work as part of an alignment check with the Blueprint (via ArB) and other potential impacted related or downstream domains (e.g., public health reporting)
9. Final Solution View documents are prepared, and any required changes are integrated into official enterprise architecture documents and/or Blueprint (approval by ArB)
10. Development of Technical View documentation commences (e.g., FHIR Implementation Guide, OpenAPI documentation, Swagger, or other technical artifacts appropriate for implementation)
11. Specifications are updated in the Blueprint technical architecture sections where needed

The proposed governance structure for the ongoing development of the platform is shown in Figure 36.

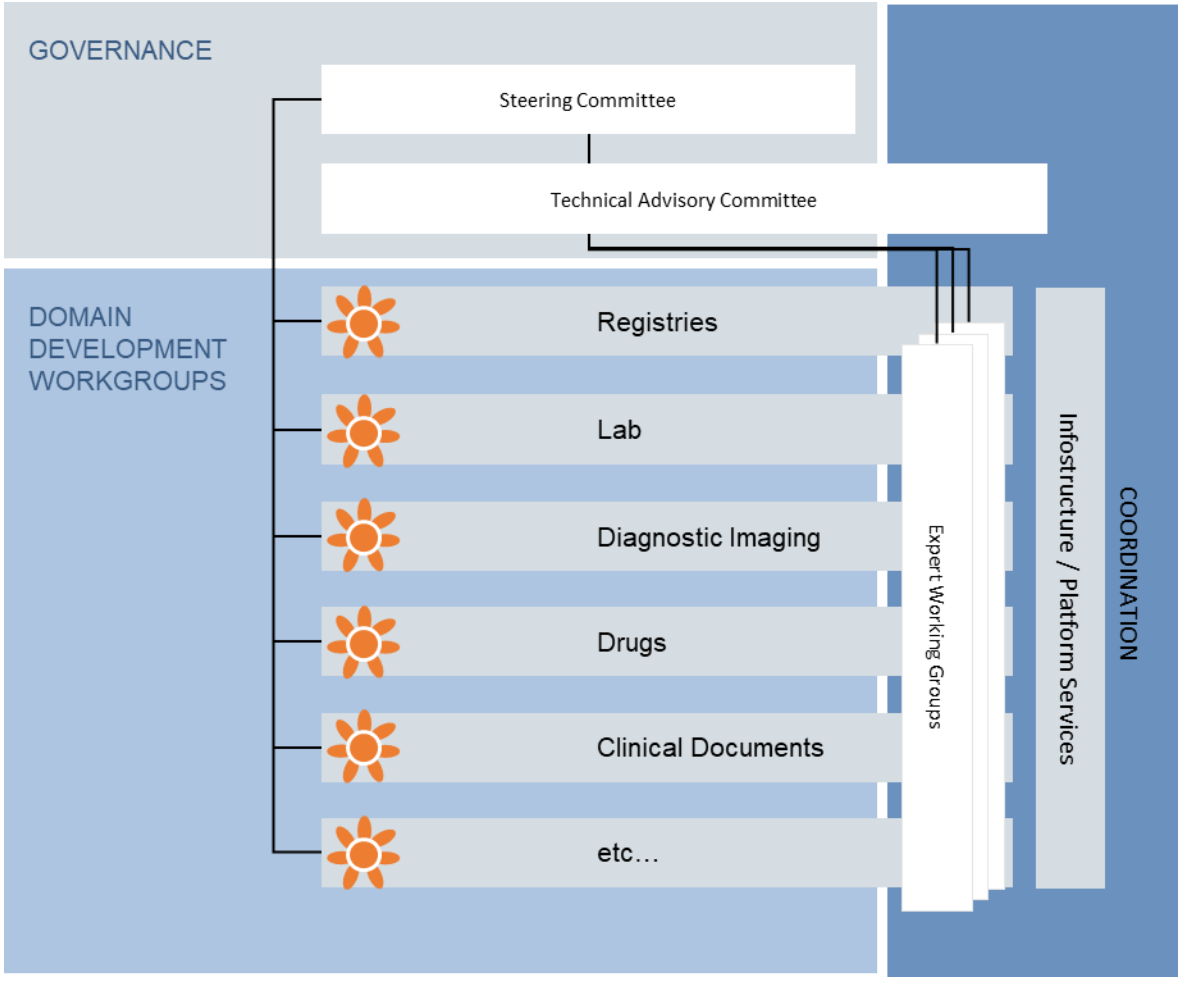

Figure 36- Domain Development Governance Structure

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 37). 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.

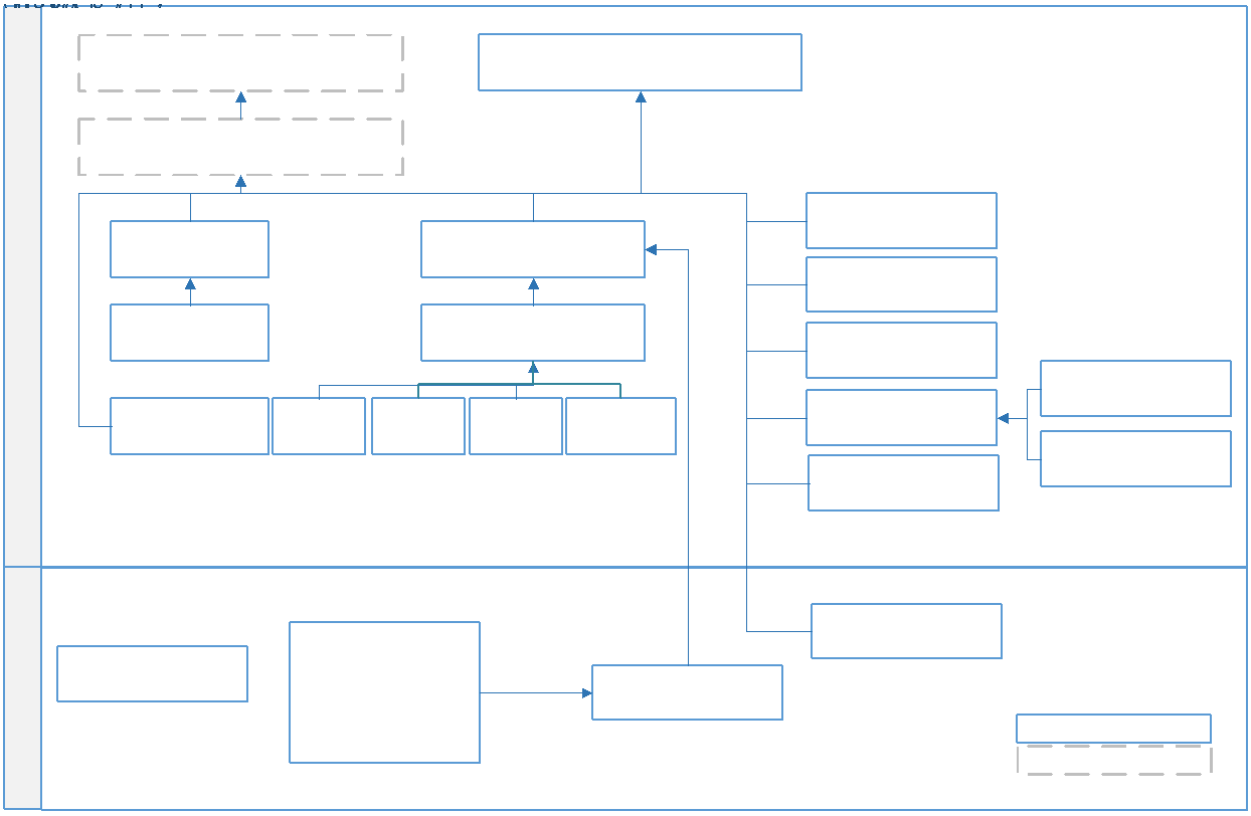

Figure 37- Baseline Information Architecture

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) 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.

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.

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 38 provides an illustration of the high-level enterprise entities considered for management within the DHP and logical relationships to one another.

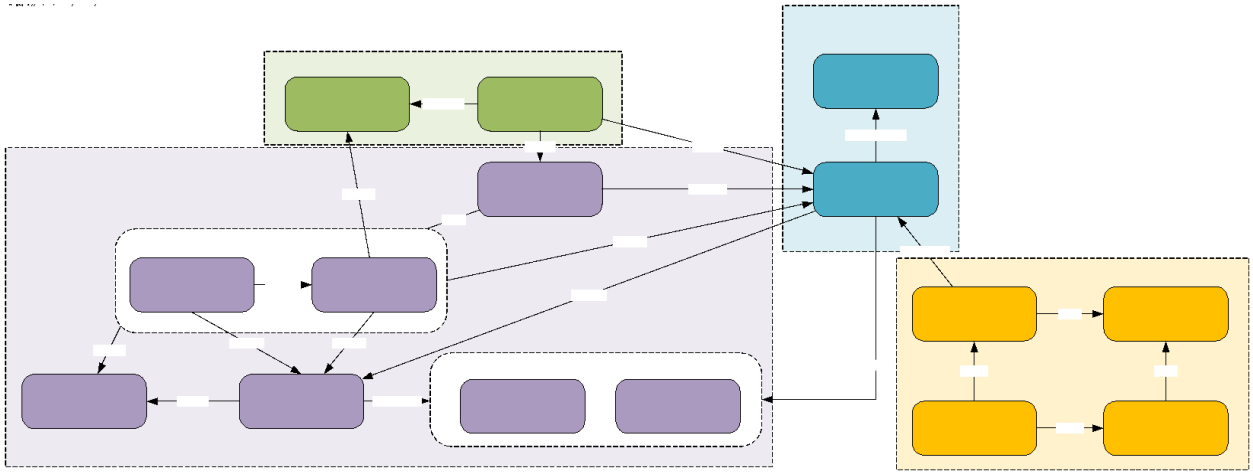

Figure 38 - Enterprise Data Entities and Relationships

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

Entity	Description	Service(s)	NDHGS 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 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.	Provider Registry	
Location / 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	
Medication / Drug	A substance which can be prescribed, administered, or dispensed to a patient.	Medication / Drug Registry, Inventory and Logistics Data	
Event	An event which should, will, did or did not occur to the patient which is 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,	KPI Repository	

	or indicators which are collected manually from health institutions via surveys.		

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 39.

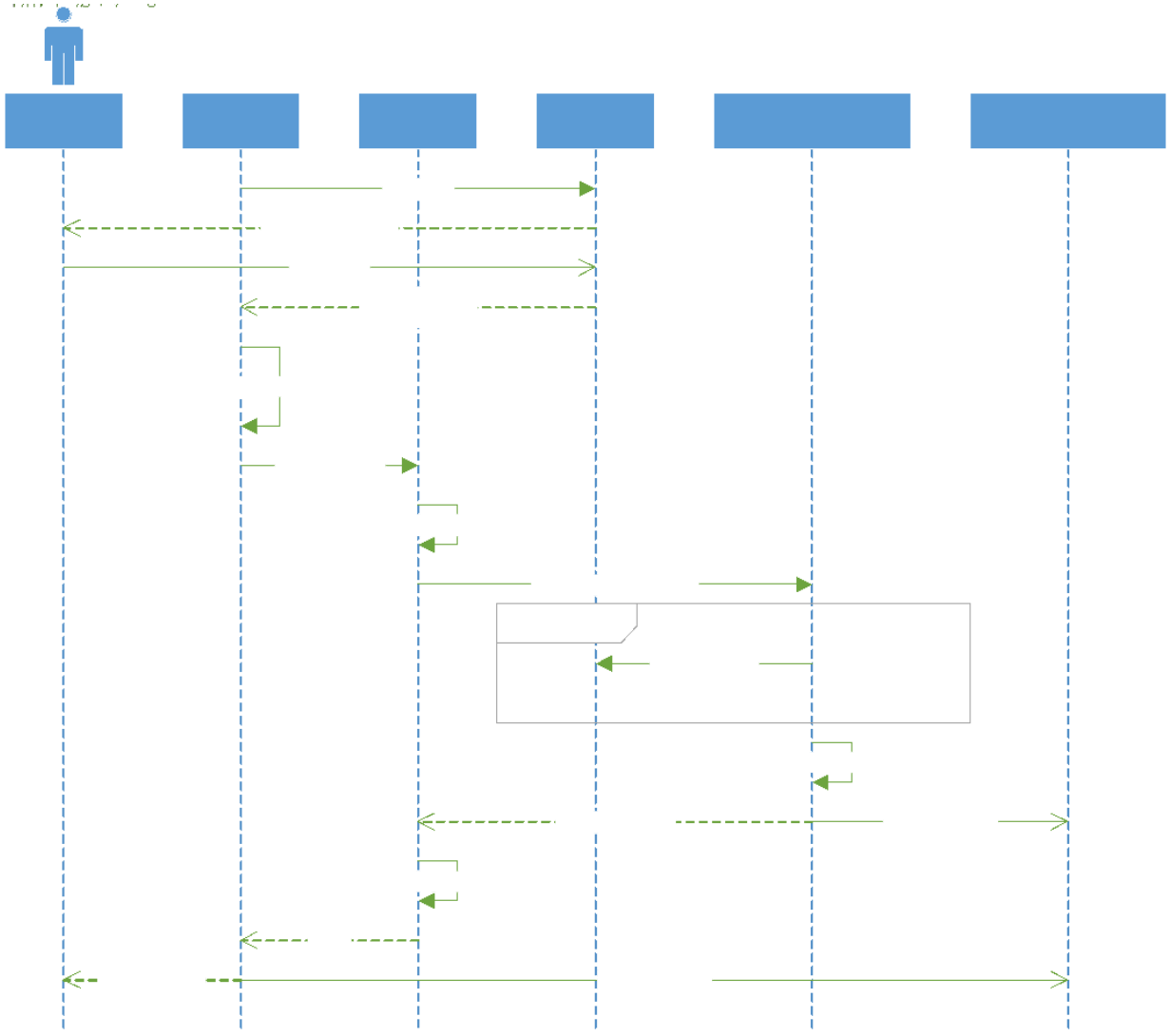

Figure 39- General Information Flow of Data Through the DHP

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)[118]
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 payload
4. The NHDX will perform necessary on-ramping / receive mediation such as:
    a. Upgrading the message format (if needed)
    b. Validating the message structure
    c. Validating the API access for the requesting system
    d. Logging the message receipt and identification
    e. Notifying subscribers of the message receipt
    f. 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 needs 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 may include:
    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 may perform whatever business function it desires.
10. The Point of Service application SHOULD audit that the operation was executed 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

[118] IUA (ihe.net)

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 40.

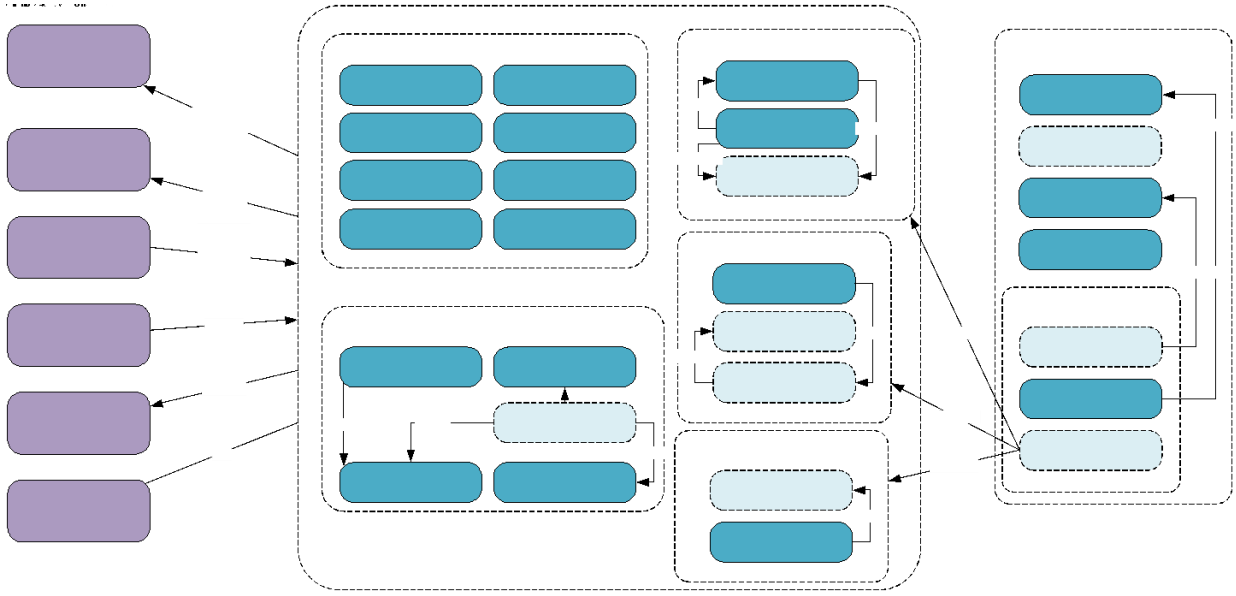

Figure 40- Event Information Model

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 Logistics and Inventory Data

The conceptual information model for the logistics and inventory domain is illustrated in Figure 41. This model is an abstraction of various models for inventory transactions[119],[120] and is provided for context of the design patterns considered for the blueprint.

[119] HL7 Reference Information Model

[120] Pages - Business Information Entities Details (gs1.org)

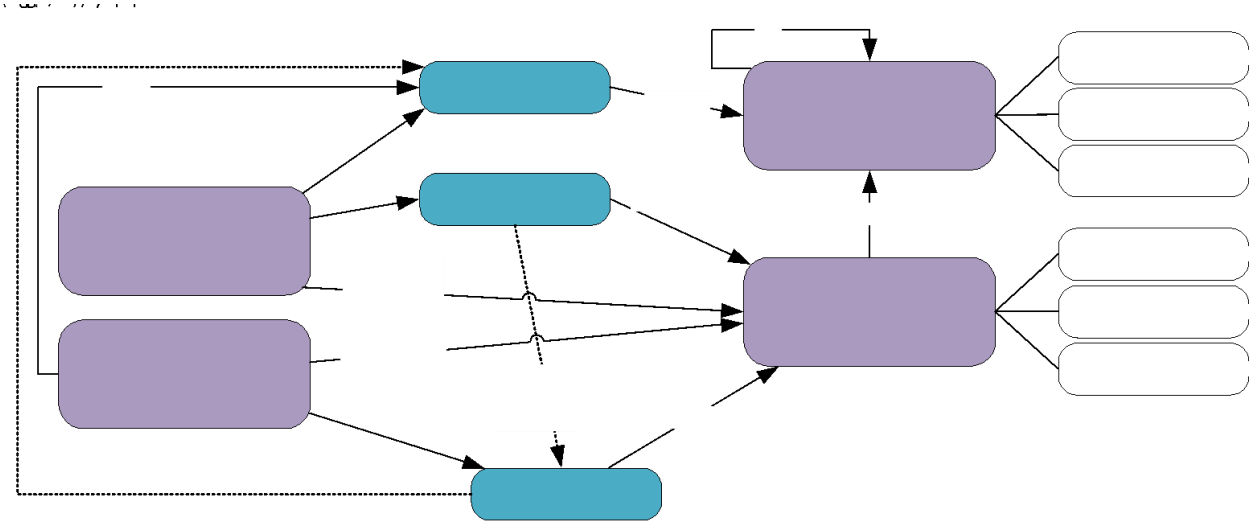

Figure 41- Logistics Conceptual Information Architecture

The entities described in the logistics and inventory model are:

- A *Supply* (trade item, or material) is a general classification of a type of item. The purpose of this abstraction is to allow for classification of the "kind" of materials which may be used, prescribed, etc. The attributes for a supply are envisioned to be used for classification, intended use, codifications, etc.
- A *manufactured supply* (transactional trade item or manufactured material) is an instance of a supply. The ability to separate the supply from instances of that supply allows orders or CDSS instructions to be recorded against a class or type of supply and fulfilled with a particular instance of the supply. Manufactured supplies carry attributes such as trade or brand name, packaging (5 dose vial, 10 capsule package), dosing, global trade identification number (GTIN), lot number, manufacture date, and expiration.
- An *order*[121] is a request made by a facility to a particular supplier such as the MOH distribution centre (or an open order to any supplier) for a specified quantity of supplies. The order is placed against the classification of item or item from a manufacturer where the supplier can fulfil the order as specified.
- A *despatch advice* record[122] is used to document the despatching (shipping) of a particular quantity of items. Despatch advice may indicate the quantity and specific GTIN (global trade identification number) and lot# of supplies shipped to the requesting facility.
- A *receive advice* record[123] is used to document the receipt of the shipment, including the accepted and rejected quantity for each (the receiving disposition). It is important to keep track of the receipt of objects as they may identify issues with the supply chain (i.e., rejections due to cold storage failure, breakage, expiration, etc.)

An example of how these concepts relate to one another is illustrated in Figure 42. In the example, a facility (Good Health Hospital) has ordered 100 doses of any SARS-COV-2 vaccine approved for use. The

[121] Pages – Order - Business Messages Details (gs1.org)
[122] Pages – Despatch Advice - Business Messages Details (gs1.org)
[123] Pages – Receiving Advice - Business Messages Details (gs1.org)

supplier organisation (in this case a ministry of health distribution centre) has packed and sent 50 each of an mRNA-based vaccine and an inactivated virus vaccine indicated in a despatch. On arrival, the receiving facility will verify the contents and will report the number of accepted stock items and the number of rejected stock items.

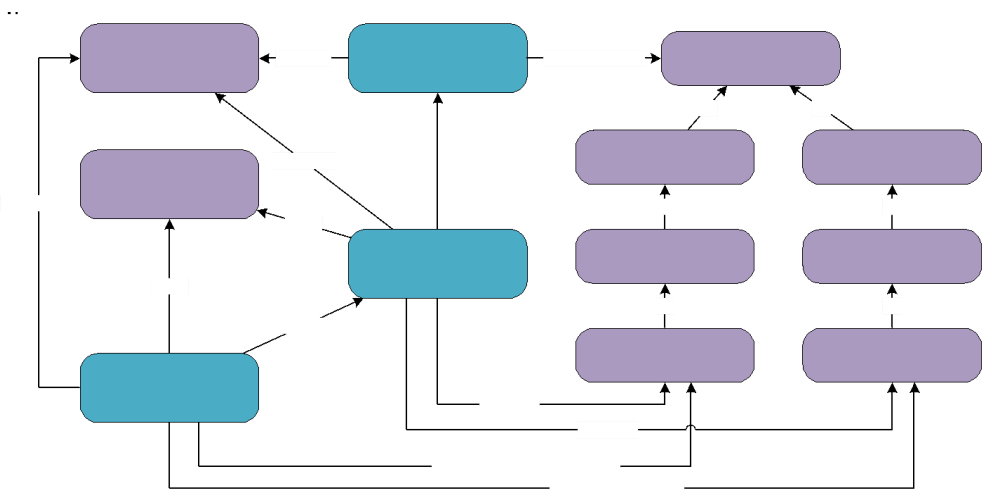

Figure 42 - Sample Relationship of Order Components

5.2.5 Security Audits

The information model for security is illustrated in Figure 43, and based on several sources include IETF RFC-3881[124], NEMA DICOM Section A.5[125], and HL7 FHIR[126].

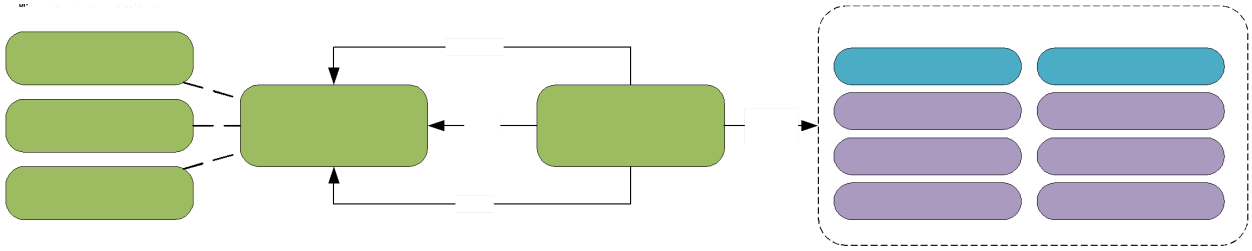

Figure 43- Logical Information Model for Audits

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:

[124] RFC 3881 - Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications (ietf.org)
[125] A.5 Audit Trail Message Format Profile (nema.org)
[126] 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 5.2.7.3 on page 145), 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

5.2.6 Secondary Use

As described in section 3.3.5.6 on page 88, 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 may mimic current information flows between disease specific programmes, and the HIMS, HHIMS and CloudHMIS to the eIMMR.

The information model of the DHIW itself will depend on the capabilities of the software used for the purpose, candidate models include:

- District Health Information System (DHIS2) as a repository of measures submitted via ADX, or FHIR Measure Reports
- Specially developed/designed warehousing technologies using Online Analytical Processing (OLAP) packages or relational databases using standardised schemas (such as the Data Vault pattern[127])
- Specialised FHIR based repositories of MeasureReport and Questionnaire Response resources

5.2.6.1 Secondary Use Information Flows

5.2.6.1.1 Submission of Aggregate Data

In this pattern of information flowing, 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[128] definition).

[127] What is "The Data Vault" and why do we need it? | Talend Cloud Integration | Talend
[128] Measure - FHIR v4.3.0 (hl7.org)

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.

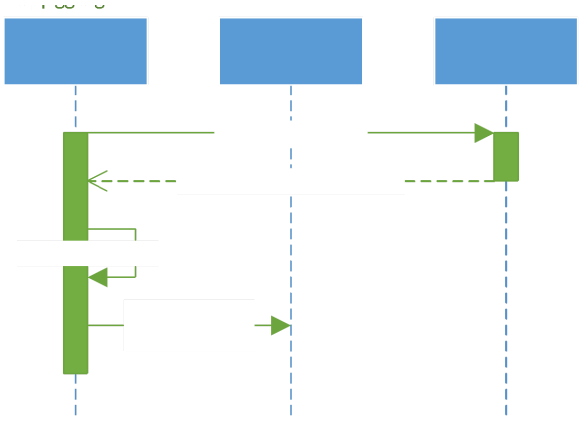

Figure 44 - Automated Aggregate Data Exchange Pattern

This information flow may use ADX[129] , HL7 FHIR MeasureReport[130] resources. There

5.2.6.1.2 Submission of Questionnaires / Surveys

This method of data capture within the DHP is aligned with current manual data capture of indicators within Sri Lanka for programmatic and surveillance tracking. In this pattern, a central repository of surveys (in FHIR parlance Questionnaires[131]) is obtained by a compatible digital health solution.

A user then completes the survey for the reporting period and submits the completed survey (QuestionnaireResponse[132]) to the NHDX for population of data within the DHIW.

[129] Aggregate Data Exchange - IHE Wiki
[130] MeasureReport - FHIR v4.3.0 (hl7.org)
[131] Questionnaire - FHIR v4.3.0 (hl7.org)
[132] QuestionnaireResponse - FHIR v4.3.0 (hl7.org)

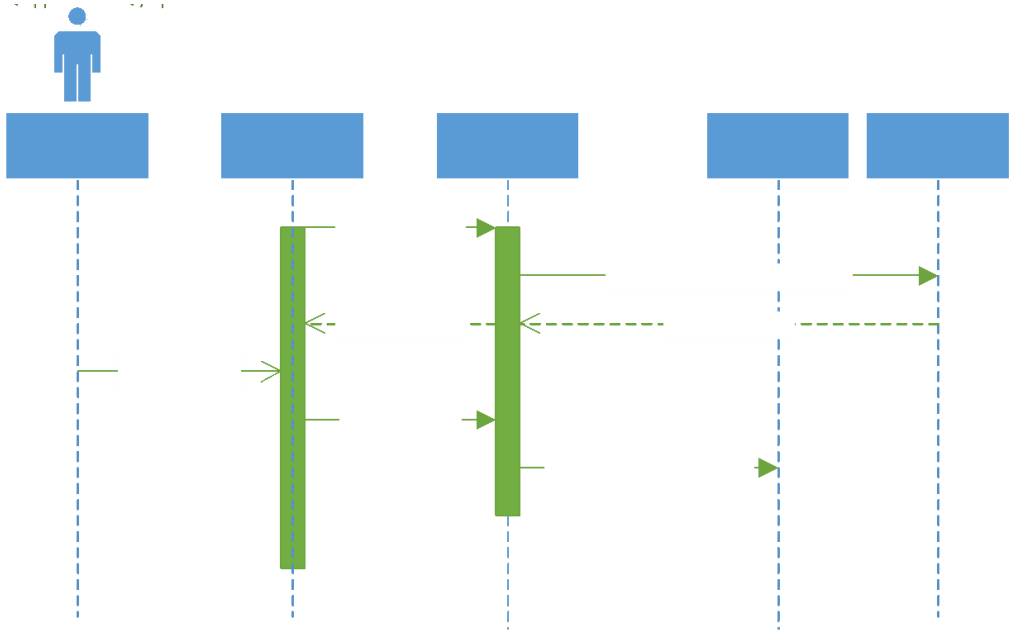

Figure 45 - Survey Population of DHIW

5.2.6.1.3 Extraction, Transform, Load (ETL)

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

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.

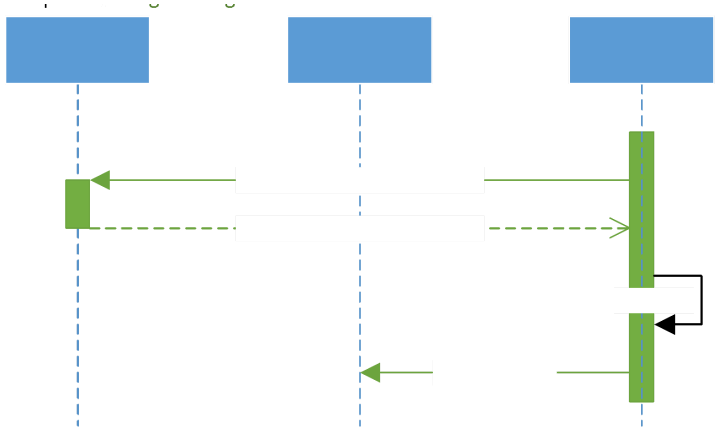

Figure 46 - Using ETL to Populate DHIW

5.2.6.1.4 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 COVID-19 infection is registered notify epidemiology unit and relevant MOH office.

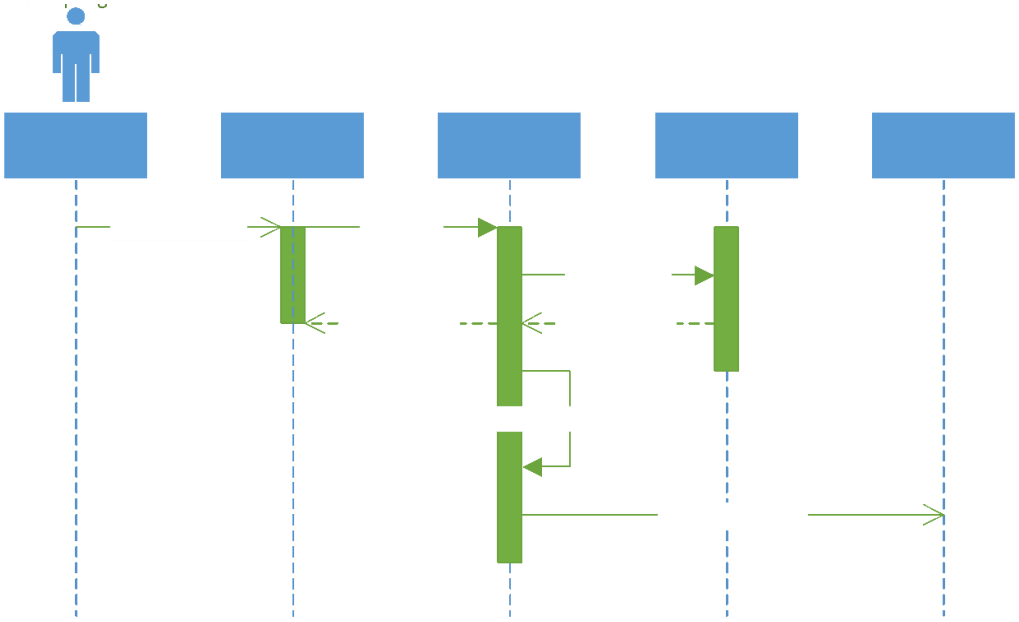

Figure 47 - Near-Real-Time Reporting

The blueprint does not prescribe the method of management for subscriptions, however a mechanism similar to the FHIR Subscription[133] can be used. The notification of the backing system (in this case the DHW) is a rest hook or push notification target.

5.2.7 Information Management Principles

5.2.7.1 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).

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

- *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[134]). 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 162.

5.2.7.2 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[135] on a resource, whereas DICOM objects use metadata elements[136]. 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.

5.2.7.3 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.

IETF RFC3881[137] provides a complete series of states for the lifecycle of health information, and a useful subset is summarised in Table 3.

Table 3 - 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

[134] Valueset-security-labels - FHIR v4.3.0 (hl7.org)
[135] http://hl7.org/fhir/resource.html#Meta
[136] 7 Registry of DICOM File Meta Elements (nema.org)
[137] RFC 3881 - Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications (ietf.org)

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 may 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.
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.

5.2.7.3.1 De-Identification

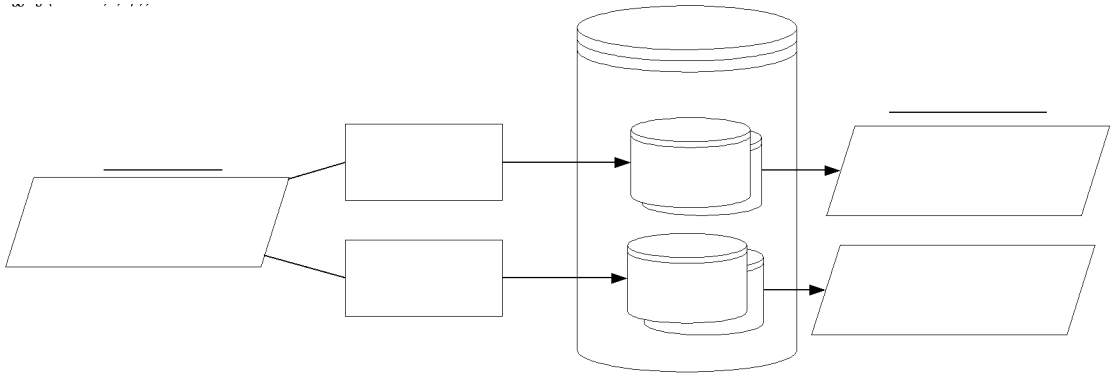

Figure 48 - Data Flow for De-Identification

Whichever techniques are employed however, de-identified data can still be full of identifying information and may 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[138].

5.2.7.4 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 may degrade over time unless care is taken to prevent this.

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

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

- 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[139]
- 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[140].

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 158)
- 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[141]
- Store and reproduce the entirety of the resource/record text (i.e., structural data will be unavailable, but in-context narrative is available)[142] when queried, so that a human reading the information can be provided a complete context of the event which occurred.

[139] Http - FHIR v4.3.0 (hl7.org)
[140] Services - FHIR v4.3.0 (hl7.org)
[141] References-definitions - FHIR v4.3.0 (hl7.org)
[142] DomainResource - FHIR v4.3.0 (hl7.org)

6 Technology Architecture

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 may be non-conformant to the Enterprise Architecture Blueprint.

The following Principles are intended to guide the development of the Blueprint components:

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.

The goal of the security design of any component in the digital health platform is to adhere to the concept of confidentiality, integrity, and availability, otherwise known in security as the CIA triad. These three fundamental considerations will form the cornerstone of the security approach for any design.

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 authentication architecture where possible. Regional or domain specific data hubs may 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.

Data in all technology solutions should be encrypted at rest and in transit. 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[143] wherever possible. Implementations shall make use of Free/Libre and Open- Source Software (FLOSS)

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

where available[144]. The platform should provide Open Data for research and quality improvement to authorized parties where suitable. Projects will utilize Open Innovation techniques when available. Applications will provide Open APIs to authorized parties where suitable.

Solution Views and guides should specify open standards and platform independent protocols to provide long term stability and interoperability. 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.

6.1.3 Interoperability Focus

Sri Lanka seeks to improve the care of patients and increase visibility into the health system on an inter-application, inter-provincial, and inter-agency basis. It is therefore important that 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.

The digital health enterprise blueprint and derivative solution guides will leverage open technical and business standards to ensure consistent processes, data capture, and terminology across software applications and organisations. 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.

Ensuring that common technical standards are in place (security, data capture, protection, etc.) is necessary to facilitate data transfer between systems. Common business processes will be included and defined in the solution views of the enterprise architecture. Common technical standards, minimum data sets, etc. will be defined in the solution views and technical views of the enterprise architecture to ensure maximal interoperability.

6.1.4 Re-Use Shared Business Services

The digital health enterprise blueprint will foster the use of centralized shared services to perform common enterprise business functions where possible. The healthcare providers of Sri Lanka deliver a variety of services to organisations, clinicians, and patients across the nation in many different and complex health domains. 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. Structured data registries, repositories, services and a “sole source of truth” will be provided where possible. Repositories will be available for patient centric health domains

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

such as labs, medications, and imaging as well as other health data such as discharge reports, referrals, etc. Shared service development will reduce the duplication of systems, promote common workflows across the enterprise and reduce point-of-service orchestration, moving toward an economy of scale. Services designed for the digital health solution should not be defined using microscopic views such as data management, rather they should be defined based on enterprise business objectives. The Blueprint will define common, logical building blocks which foster easy sharing of enterprise business functions across system boundaries. Each identified Domain should be further specified in a Solution View and Technical View.

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 / 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.

6.1.7 Use of Building Blocks

Solution designs should promote a building block approach, incorporating “loose coupling” and “high cohesion” into designs.

Loose coupling of services and applications allows stakeholders and participants to interchange or swap existing implementations for new or more appropriate solutions whilst not introducing cascading changes to other components. Said another way, changes in one component have minimal effects on the existence or performance of another component. For example, the strategic use of APIs allows for re-use of business components across applications, mobile apps, portals, and web services workflows. Loose coupling also allows for smooth versioning and service migration between releases of standards.

High cohesion refers to the degree to which the elements inside a module belong together. Cohesion aggregates common functions and business processes together within a conceptual building block. Each service component should encapsulate all necessary functions to perform the business processes defined (for example: The Master Patient Index should not be considered the authoritative source for Facility Data). Each building block should be implementable, independently useful, and reusable across

functional areas and use-cases where possible. Building blocks should be internally interoperable by design.

6.2 Functional Principles of DHP Building Blocks

This section introduces the minimum common functional principles of any component 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 may be 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.

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

Figure 49 – Non-Repudiation of Emission

Additionally, 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.

Figure 50 - Non-Repudiation of Origin

These three principles, when used in coordination with one another, ensure that data submitted to the enterprise is:

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

An example of how non-repudiation can be implemented in a message being sent to the health infostructure is illustrated in Figure 51.

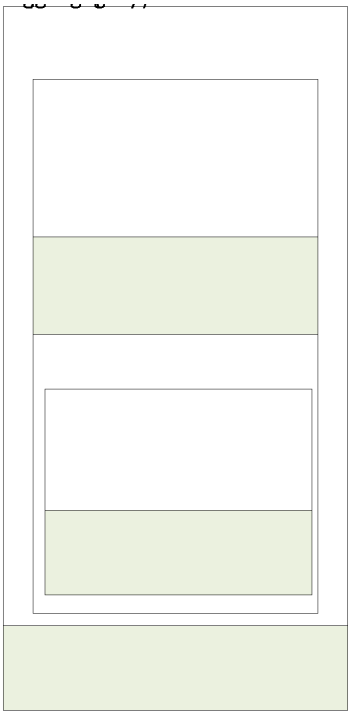

Figure 51 – Example of implementing Non-Repudiation in an SOA Message

It is recommended that clinical payload data be signed separately from the overall message since it is quite common for the message exchange infrastructure to modify message headers during processing. Signing the overall message provides proof of the original form of the message that was submitted to the infrastructure.

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. Enterprise identifiers should be meaningless but unique numbers (commonly referred to as MBUNs). Enterprise identifiers must be comprised of at least two parts – a system source identifier and an entity identifier. Local identifiers should not be shared or stored outside of the source enterprise if possible.

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.

These identifiers should include both the identification number and the identity domain in which that business identifier resides. This combination of identification number and identity domain will ensure that the DHS can unambiguously determine what the identifier points to. Alternately, solutions may choose to implement a scheme of universally unique identifiers (UUID).

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.

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

6.2.4 Follow Standards and Interoperability Plan

Implementations of the services in the DHP will follow the Interoperability Plan for Sri Lankan digital health standards wherever possible[145].

Solutions Guides (see section 2.3.2 on page 32) will define:

- Trigger events which define when the point of service applications may contact the shared DHP infrastructure, or when DHP services may be contacted
- 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)

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

6.2.5 Encapsulation of Data Submitted

Whenever submitting data to an enterprise, the contents of the message may be transmitted, wrapped, change representations (XML or JSON), may be queued and retried, etc. Because of this, it is highly recommended that DHP services and point of service applications develop business level services (see Figure 11– Solving Problems using a SOA Approach) and do not rely entirely on simplistic representational state transfer (REST) CRUD (Create, Read, Update, Delete) methodology when creating or updating data.

Atomic transactions such as CRUD lack transactional control and often lack sufficient context (for example: when accepting HTTP requests and storing them for retry in a JMS queue). Atomic transactions also lack supporting data required for cross referencing and validation (patients, facilities, organizations, etc.), the clinical rationale for the transaction (example: create patient because of birth event, update patient because of death). It is also rarely appropriate for a point of service application to instruct the digital health platform to modify data in the DHP directly without appropriate business rule processing.

Atomic transactions should likely be restricted to READ operations for POS systems and higher-level business interfaces (APIs) should be developed for interactions that insert or modify data in the DHP.

As a general guideline to address these challenges, interfaces and APIs which are used in the DHP should:

- 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 the dependent objects which are referenced in the clinical act including patient demographics, provider demographics, facility information, etc. For example, instead of submitting a FHIR observation as a standalone resource, a bundle which includes patient demographics, provider demographics, facility information and the observation should be submitted.
- 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[146].

6.2.6 Performance Targets

There are more than 1,600 institutions in the public curative sector 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 in line with clinical business processes.

6.2.6.1 Performance of DHP Services

DHP services may 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 24x7x365 with greater than 99%

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

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 may be used in cases where a network 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 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, implementers should adhere to the patterns described in 4.2.2.5.1 on page 96.

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 of Devices, Users, and Applications

Services which comprise the DHP may 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[147] "…any party in possession of a bearer token "(a "bearer") can use it to get access to the associated resources (without demonstrating 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) as well as centralised authentication of users. 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:

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

    - 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 may 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[148], and OpenID Connect for application and user authentication[149]. There may be multiple issuers of identities trusted by the central DHP (federated by public/private, or provincial boundaries).

6.2.8 Authorisation of Security Principals and Services

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 (for example: a client registry may have different authorisation requirements than the national EHR). The authentication token and authorisation of that token to scopes may 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:

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

[148] IHE ITI TF Vol2 – ITI-19 Authenticate Node
[149] OPENID Authentication Flows (hidglobal.com)

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[150]. 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 solution 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 will be performed on all connected digital health services prior to issuance of a device or application credential[151,152].

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 may be used to store documentation (or directives) of the patient in relation to the use of their data in the DHP. The XML Access Control Markup Language (XACML)[153] architecture components should be used as a framework for enforcement of consent directives within the DHP. The architecture is summarised in Figure 52:

[150] National Digital Health Guidelines and Standards [2] Section 6.3.3
[151] National Digital Health Guidelines and Standards [2] Section 3.1.10
[152] National Digital Health Guidelines and Standards [2] Section 6.3.12
[153] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

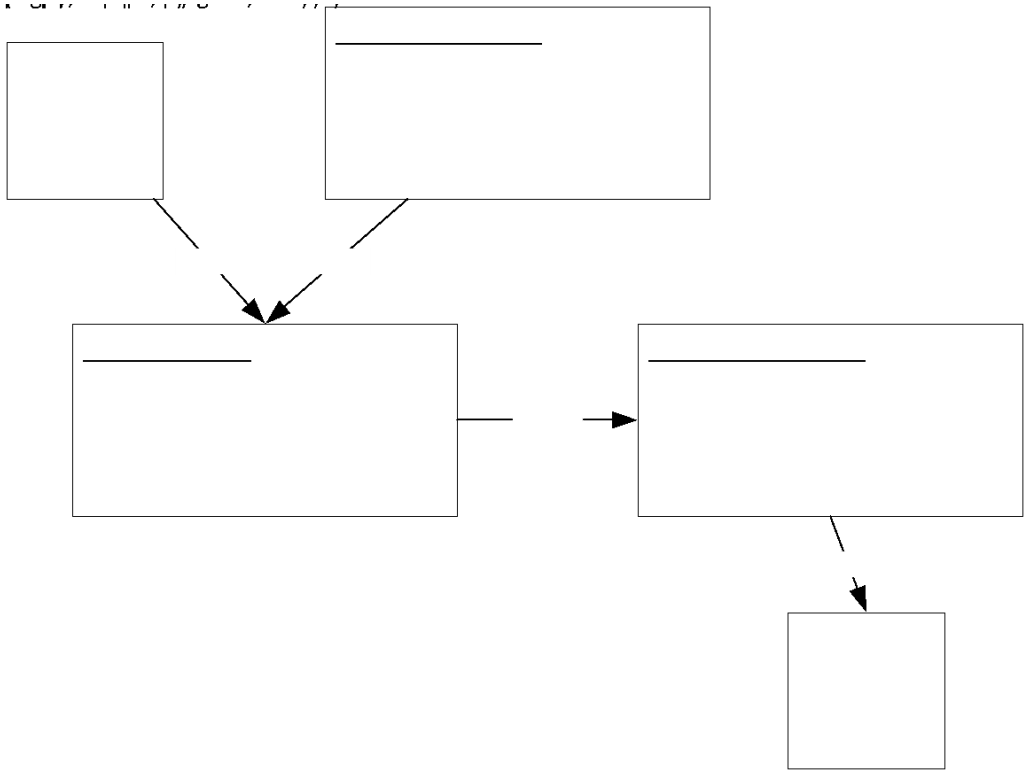

Figure 52 - Policy Information, Decision and Enforcement

- *Policy Information*: In the DHP policy information related to consent and disclosure of data should be stored in the consent directive repository. This repository should include:
    - A list of access policies in the enterprise
    - An association of policies with actors (i.e., patients, and users) or data (i.e., clinical data, administrative data).
- *Policy Decision*: In the DHP the policy decision may be performed by the identity provider to establish a list of scopes for a user session or may be a shared service (this is like a XACML Policy Decision Point service) which is responsible for applying the configured policy definitions against a disclosure or access request.
- *Policy Enforcement*: In the DHP, policy enforcement should be performed by the DHP service (such as client registry, national EHR, etc.) to take context appropriate action. Actions may 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 may 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 (i.e., requires no mediation) or orchestrated (i.e., requires mediation services).

To support this function, all messages submitted to the DHP must contain in appropriate message wrappers:

- The originating organisation and facility
- The application instance which generated the information (e.g., HHIMS version 1.5.3 running at Good Health 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)

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 may be 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 may occur.

Consider, for example, a PoS (for example: HHIMS) contacting the DHP to post a document. Such a transaction from the point of view of the PoS is opaque, however the DHP may rely on the orchestration of several services to achieve the business goal (illustrated in Figure 53).

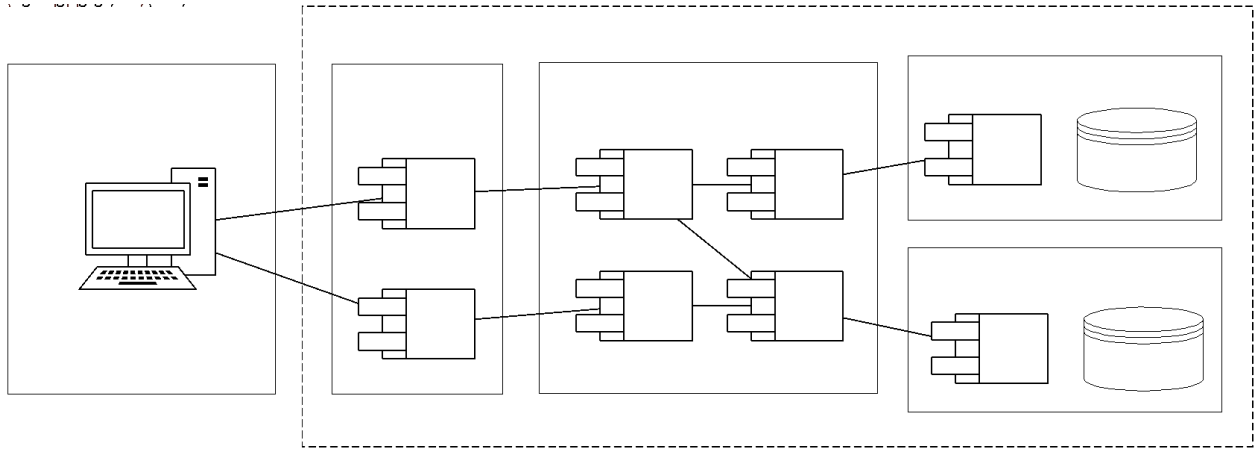

Figure 53 - Service Orchestration and Composition in the DHP

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 OperationOutcome[154] 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:

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

    - 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 may decide on appropriate action which may 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

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"[155] 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[156] (ESB), it is expected that the integration layer (the NHDX) persists information about the exception it has received from a service.

[155] Implementing Exceptions in SOA (infoq.com)
[156] 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[157] 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. This means introducing and expanding digital devices and systems, electronic forms, and data capture throughout administrative and clinical processes. This is also the first step to workforce digital literacy and capacity building and involves on-boarding as many users as possible to utilise digital technologies in the clinical environments on a daily basis.

7.1.2 Connecting Digitised Solutions

The next (or preferred, in parallel) stage of digital evolution is to begin to connect people, institutions, facilities, and systems. 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/consumers and clinicians in the extended circle of care, as

[157] Adapted from: Parker, Ron. Enabling Coordinated and Collaborative Health Care. Canada Health Infoway, 30 March 2016. Webinar.

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 national vaccination forecasting application can 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[158], “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 deployed as resources become available, growing organically as more infrastructure and components are built and as more external applications are

[158] 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/

connected. As implementations mature, specifications will evolve, functionality will grow, and the health system of Sri Lanka will begin to transform.

7.2 Prioritised Action Plan

The following section lays out a plan of action in priority sequence to begin the Blueprint realisation in Sri Lanka.

The initial plan in described in three timeframes: Immediate, Short-term, and Medium-term. Immediate term actions are intended to be started as soon as the program has been resourced. Short-term initiatives should begin within 12 months of the Immediate term actions, and Medium-Term activities should begin within 24 months of the start of the program.

The summarised action plan is outlined in Table 4.

Table 4 - Prioritised Action Plan

Timeline	Action
Immediate (upon program initiation) **Stages: Digitising, Connecting**	1. Establish Project Management Office (PMO) for governance and oversight. Develop organisational structures and begin policy development. Develop procurement plan 2. Procure wired & wireless networking equipment, laptops, and workstations 3. Procure equipment for hosting and expansion of existing Hospital Information Systems (HIS) at prioritized hospitals and clinics 4. Establish secure connectivity and backup wireless connectivity for networks involved in care delivery 5. Establish secure cloud hosting environment for NHDX, including identity provider service. Provision secure communications services for providers 6. Begin design, development, and implementation of NHDX interoperability layer and components (e.g., Client Registry, Provider Registry, Facility Registry, National Reporting Systems, etc. - see dependency map for sequencing) 7. Begin upgrading of functionality & expansion of existing HHIMS system 8. Begin formulation of the standard operating procedures (SOPs), advocacy, capacity building, site visits, audits, and research related to health information system governance 9. Establish Health Information Management Units (HIMU) in selected hospitals to support governance and implementation activities 10. Develop communications plan for promoting activities 11. Engage public and private sector stakeholders 12. Establish a national help desk to attend to the issues regarding HIMS implementation and operations

	13. Establish at least 5 Provincial Training Centres. Begin training of clinical staff on basic ICT literacy and HMIS specific functions 14. Procure training for technical staff on how to design and link DHIS-2 based modules to the central HMIS API
Short-term (begin within 12 months) **Stages: Connecting, Sharing**	1. Procure and implement foundational components of NHDX (vocabulary service software, etc., see dependency map for details) 2. Begin assessment of legacy point-of-service systems for adoption of standards and integration into NHDX (HIV, TB, Primary Care, Ambulatory Care, etc.) 3. Begin design, development, and integration of point-of-service systems to NHDX (HIV, TB, Primary Care, Ambulatory Care, etc.) 4. Integrate clinical supportive technologies such as lab analysers into local hospital information systems 5. Incorporate the ICPC-2 and ICD-10 coding systems in all critical systems with built-in cross-mapping between the two coding systems 6. Begin design and development of priority NHDX applications (e.g., eReferral, Patient viewer portal, Personal Health Record with mobile access etc.) 7. Implement operational supports such as national digital health service desk and network, security, and privacy operations centres 8. Develop additional digital health training modules 9. Design and implement health information warehouse, reporting and analytics system
Medium-term (begin within 24 months) **Stages: Sharing, Informing**	1. Expand training and capacity building activities 2. Conduct data validation activities 3. Develop key performance indicators (KPIs), service level agreements (SLAs), and implement performance management system for long term management 4. Conduct surveys to collect feedback from users and clinicians 5. Develop, test and document disaster recovery plans 6. Continuous integration with strategic systems

Figure 54 - Prioritised Action Plan

The action plan described above will likely consist of several workstreams proceeding in parallel, beginning with the fundamental move to electronic and digital platforms by deploying secure digital networks and devices wherever possible. This will provide the fundamental underlying connectivity required for all future development, including backup mobile connectivity to the health data centres of the hospitals to maintain the reliability of the health information systems.

This workstream will design and procure networks & secure connectivity, create specifications, and begin development of HHIMS system upgrades, procure a strategic cloud hosting environment, and may choose to establish standards for devices such as desktops, laptops, tablets, and phones. This phase will likely purchase hardware for priority areas such as patient registration, clinical workstations, nurses' stations, radiology workstations and networking, and will purchase local servers for decentralised HHMIS hosting at major hospitals where applicable. This phase should also seek to establish relationships for local technical assistance on process management, enterprise architecture, business analysis, database administration, and software developers.

An early workstream in the programme management office (PMO) should also seek to establish privacy & security policies & develop guidelines and templates for processes such as privacy impact assessments (PIA) and threat risk assessments (TRA) for forthcoming projects. This workstream should begin to consider future organisational structures and operating units such as Helpdesk, Security Operations Centre (SOC), Network Operations Centre (NOC), Privacy Operations Centre (POC) and their roles & responsibilities, locations, and structure (e.g., centralised / de-centralised), as well as a preliminary staffing & support model to support platforms and applications. Most importantly, this workstream should seek to understand any regulatory barriers, legislative or policy changes that may be required to move forward with the implementation of the digital health platform, for example any data sharing agreements or cross-institutional policies that will need to be developed.

A workstream that should be conducted during the immediate stage of work is the establishment of working groups to create the Solution Views and Technical Views for the NHDX interoperability layer design which will define the detailed standards and functionality each business domain. As described in section 2.3 Architectural Views (Enterprise vs. Solution vs. Technical) (on page 29) of this document, the Blueprint and National Interoperability Plan convey the *conceptual level* of the digital health architecture. From this, multiple Solution Views (logical level) and Technical Views (physical level) must be derived. For example, for each business domain identified (e.g., Patient Administration, Provider Registry, IT Infrastructure, Consent Management, Shared Health Record, Analytics, etc.) these Solution and Technical artefacts must be developed. The domain list should be prioritised using the dependency map, and artefacts will be developed in priority order. It is recommended that the first domains to be developed will be IT Infrastructure and Patient administration, due to the fundamental and highly dependent nature for other domains.

For example, patient administration will describe in detail the workflows and business rules for using the national personal health identifier. Once these domains views are established, it will be possible to design interoperable clinical applications (e.g., a referral system from hospital OPD secondary care using the HHIMS, OpenMRS and HIMS information systems for referral management via enterprise service bus and the implementation of the above in the hospitals.

Fundamental topics such as authentication, authorisation, audit etc. will be covered in IT Infrastructure domain, and APIs will be described in detail in the technical view documents for each domain. It is

important to note that every domain need not to be completed (or even started) before one of the earlier domains moves forward with implementation, allowing for an agile, incremental implementation. Designers should use the included dependency map to assist in prioritising system design activities.

Early integration projects should include an activity to establish an application programming interface (API) standard to include data from diverse clinical information systems. This includes integrating the private sector to the national level reporting systems, especially in primary care/ambulatory care where data feeds should be established to collect outpatient care data from public and private healthcare institutions. Interfaces to the three disease program information systems (TB, Malaria and HIV) should also be designed, built, and implemented to allow data sharing with the main HMIS. Integration with other public health information systems should be undertaken gradually based on the priorities set by program governance.

7.2.1 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 “swasthatha”.

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 7.3.1).

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 / Pilot an e-referral solution leveraging the blueprint infrastructure (example: between OPD and hospital systems)
    c. Establish / Define standards-based APIs and integration profiles in line with the blueprint between private sector and public sector institutions to the national level.
    d. Develop / Pilot the integration of information from disease program information systems with HHIMS using the NHDX and/or NEHR functionality.
    e. 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).

7.2.2 Interoperability Plan Development

As detailed in the blueprint (section 2.3.2 on page 32), 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.

Based on the initial set of projects underway in Sri Lanka, enabling digitisation and connectivity, and the shared nature of services, an initial set of solutions views are proposed to be developed within Sri Lanka and enumerated in Table 5.

Table 5 - Initial Solution & Technical Views

Domain/Service	Solution View	Technical View
Identity Provider	Documentation of shared authentication service use-cases for central API key authentication (immediate need) and user authentication (secondary need).	Identity Provider Integration Guide (in PDF format) – Specification of OpenID Connect, JWT claims, access token requirements.
Health Provider Registry	SRS has already been developed with use cases and business descriptions for the software implementation. These will be adapted to interoperability/service definition profiles.	FHIR IG. Profile of Practitioner, PractitionerRole, Organization, HealthService. Include/reference mCSD IG[159].
Health Facility Registry		FHIR IG. Profile of Location, HealthService. Include/reference mCSD IG
Terminology Services	Initial SRS and working group have been developed/established. This will be adapted, (with references from other assets available, example: OpenHIE) into a terminology services solution view.	FHIR IG. Profile of ValueSet, CodeSystem, and ConceptMap as appropriate. Include/reference IHE SVCM[160]
Master Patient Index	OpenHIE client registry use cases and existing data model specification for software development has been created. These will be adapted to an interoperability/service definition profile.	FHIR IG. Profile of Patient, RelatedPerson, Person. Include/reference PIXm[161], PDQm[162], PMIR[163] profiles.
Audit Repository	Documentation of shared audit repository interface specification and business events.	FHIR IG. Profile of AuditEvent. Include/reference BALP[164] and RESTful ATNA[165]

[159] Mobile Care Services Discovery (mCSD) - IHE Wiki
[160] IHE_ITI_Suppl_SVCM
[161] IHE.ITI.PIXM\1:41. PIXm Home - FHIR v4.0.1
[162] IHE.ITI.PDQM\Patient Demographics Query for Mobile - FHIR v4.0.1
[163] IHE.ITI.PMIR\1:49 Patient Master Identity Registry (PMIR) Profile - FHIR v4.0.1
[164] IHE.ITI.BALP\Basic Audit Log Pattern (BALP) - FHIR v4.0.1
[165] IHE_ITI_Suppl_RESTful-ATNA

Data Health Information Warehouse	Initial series of requirements and design documents have been started using ETL based methods. These will be used as inputs into the interoperability design of the data warehousing solution.	FHIR IG. Profile of Measure, MeasureReport. Structure and processes for creating Questionnaires. Referencing ADX[166], mADX[167] profiles.

7.3 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 55 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.

[166] Aggregate Data Exchange - IHE Wiki

[167] Mobile Aggregate Data Exchange (mADX) - IHE Wiki

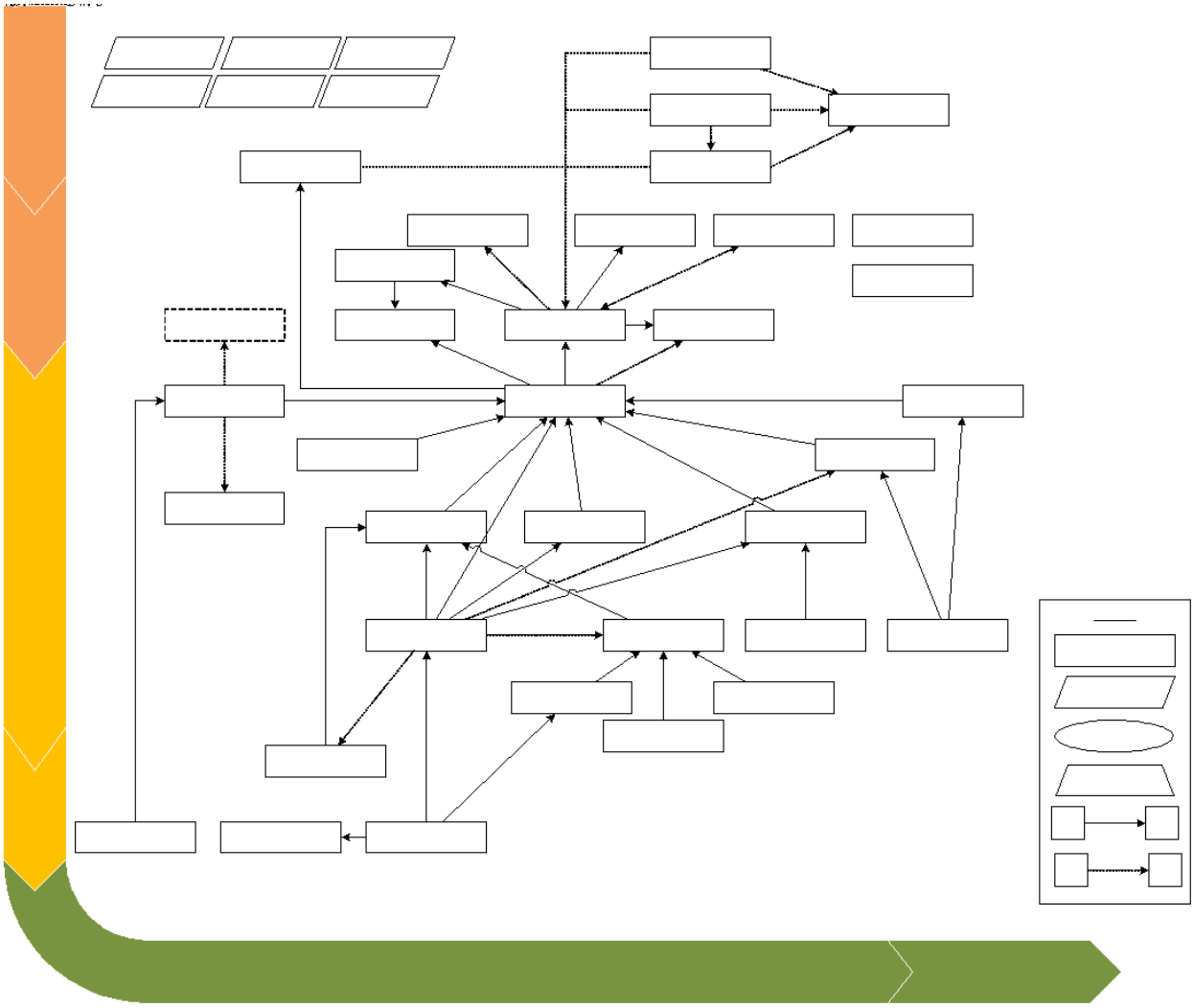

Figure 55 - Blueprint Component Dependencies

The complete dependency list between blueprint components is enumerated in 0.

7.3.1 Sample Project Dependency Map

For example, a project establishing an e-referral from hospitals using structured e-referral documents between HHIMS, HIMS, OpenMRS and Private HIS instances would rely on several services within the DHP. Using the dependency map, a project planner would see which services need to be at least partially implemented (Figure 56)

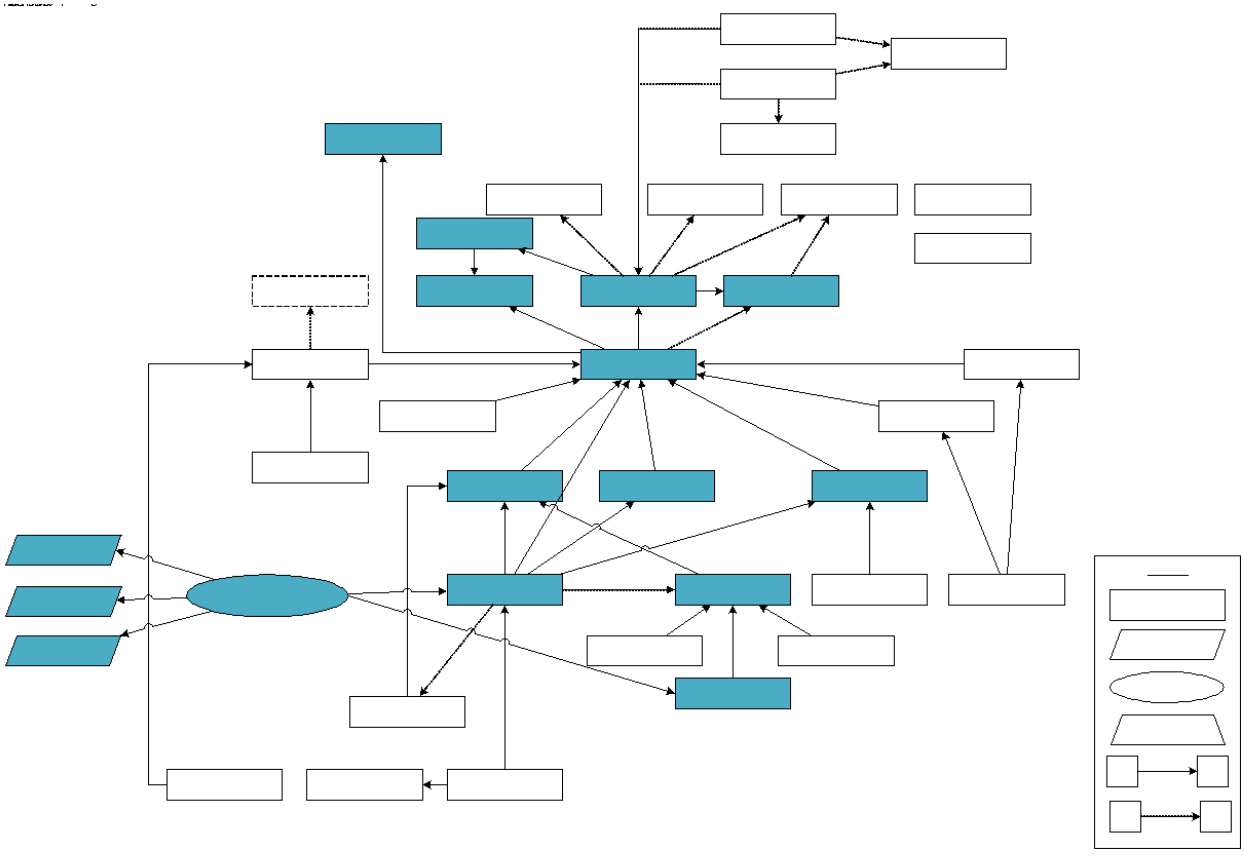

Figure 56 - Sample Project Dependency Map

For example, an e-referral project would require a subset of services from:

- NEHR Repository – To share EHR summaries between the client system software
- Master Patient Index – To establish consistent identity of the patient being referred
- Facility Registry – To establish a consistent identity of the facilities being referred from/to
- Provider Registry – To establish consistent identity of the provider organisations/workers
- Document Repository – To store the e-referral structured document
- Record Locator/Index – To link the e-referral structured document to the NEHR record
- National Health Data Exchange – To facilitate the exchange of data
- Identity Provider – To authenticate the users, and applications sharing the data
- Certificate Services – To encrypt the data in transit and at rest
- Audit Repository – To audit the creation of the e-referral, the login of providers, etc.
- Time Keeping – To ensure that all timestamps are consistent between the software solutions
- Terminology Services – To ensure the referral service codes are consistent between the systems.

7.4 System Implementation Approaches

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. This is commonly referred to as the “buy vs. build” decision.

The first approach is to use “common off the shelf” software (COTS) by applying configurations to software but no customisations that require source code changes. The second approach is to purchase subscription-based software as a managed service, normally provided over the internet (these solutions normally require greater attention to privacy and security issues as well as data residency considerations). A third option is to begin from an existing package, framework or even complete application that has previously been developed where the licensing allows for modification and enhancement (such as Open-Source software). Finally, brand new software can be designed and developed from the ground up. Each approach has benefits and drawbacks in terms of licensing costs, ongoing modifications or changes and support model.

7.4.1 Build vs. Buy

Typically, the decision to buy or build software is made for each individual system. Some general considerations to be used are: cost of the software (license + support and/or subscription), responsibility for maintenance (bug fixes, data migrations, etc.), control (changes to features over time, availability/outages if subscription based), fitness for purpose (availability of software that meets all special requirements), extensibility (can be customised or expanded as needed), scalability (can perform under anticipated loads), conformity (works well in the broader technology environment) and supportability (the organisation has the capacity and skills to support the platform and tools).

Build

- Pros
  - Highly customizable
  - Highly specialized
  - Familiar platforms and tools
  - Intellectual property rights
  - Control over changes and operations
  - Lack of external dependence
- Cons
  - Potential higher cost
  - Potential lack of specialized domain knowledge
  - Risks of timelines, quality

Buy

- Pros
  - Faster time to deployment
  - Potentially lower costs
  - Outsourced maintenance
  - Economy of scale
- Cons
  - Lack of ownership rights
  - Lack of control over feature development
  - Potential sunsetting / end of life
  - Dependence on vendor

Figure 57 - Build vs Buy Decision

7.4.2 Adopt, Adapt, Develop

One of the key cost savings in the integration of shared infrastructure comes from the strategy of adopt, adapt, and develop. In this pattern, implementation focuses on:

- Adopting existing standards, software, or technologies without any changes. Even if there are licensing fees, it can be much more cost efficient than running expensive development teams and performing full analysis, development, and testing cycles.

- Adapting existing standards, software, and technologies for the Sri Lankan context. This involves getting software and customising it for the purpose within the blueprint and can often time require less resourcing than full development and has the added benefit of global communities of expertise.
- Developing standards, software and technologies from scratch can be the most intensive should be avoided if existing solutions cannot be adapted.

7.5 Operating Environments

In a complex enterprise such as a national digital health system, several system operating environments are normally established. The industry standard is to have four working environments, which are referred to Development, Testing, Staging and Production. The development environment(s) are established and primarily used by software development and quality assurance teams. They are often transient and unstable and should not contain any real data such as personal health information. The Test environment is a copy of the software environment for testing new features, integrations or other new or modified functionality. The data in the Test environment is normally synthetic and is not a copy of real health information. The Staging environment is designed to be a very close match to the production environment. The purpose of Staging is to complete any final testing before changes are promoted to the Production environment. Finally, the Production environment is the system that is live and accessed by users for day-to-day business purposes. The Production environment hardware is scaled to support the live load for all active users and is normally substantially larger than the other environments.

Environments can be constructed on-premises in data centres located in health facilities, can be consolidated into a central data centre, or accessed remotely via third party cloud services. The choice of where to host various environments, especially the Production environment can have a major impact on the availability of the environment, especially during extraordinary circumstances such as power outages and cyber events. Newer, consumption-based subscription models can also dramatically impact the costs of operating these environments. Special attention should be paid to the environments that are required by each solution.

7.5.1 Strategic Environments

Beyond the various environments used for the ICT operations lifecycle, other jurisdictions have created additional environments for strategic purposes. Two such examples are a Reference Implementation environment and a Sandbox environment.

7.5.1.1 Reference Implementation

A Reference Implementation (RI) is a software package (or entire system) that implements a detailed specification. The main purpose of the RI is to help in the creation of other implementations of the specification by serving as a point of reference for testing (as opposed to being used in a production environment). This is very valuable when specifications are new, and few, if any, implementations of the specification are available for testing or use. The Reference Implementation can serve as a basic conformance test for new systems without requiring the security and performance overhead of a production operational system.

A Reference Implementation is not a feature complete and functioning implementation of a national digital health blueprint. Rather, it is a valuable resource to provide early-on in a national or regional program to further refine design details and to build a community of practice in the region. A Reference

Implementation is also not a tool for production system conformance assessment. Only a Production Test System or other certified conformance environment should be used to validate that health system software is behaving in a safe and fit-for-purpose way.

Reference Implementations have been seen to strengthen digital health programmes globally by removing some of the “hesitancy” of moving towards digital health solutions by providing a set of engaged stakeholders with a foundation for a common, shared understanding. The Reference Implementation enables the open, standards-based approach to co-design and highlights business, education, and regulatory requirements. The reference implementation provides an experimental working version of the DHP infostructure, providing visibility into the platform’s common components and how they work both internally and with external applications. The RI provides an environment for experimenting with international eHealth standards and will expose any local refinements that will be required in the current context. The RI design documentation begins to define the functional and technical requirements needed by systems integrators and solutions providers to build or modify digital health components and/or applications, giving them a head start on being prepared to integrate into a national system.

7.5.1.2 Sandbox Environment

Another common type of system is a Sandbox Environment. This is an environment where several participants can install their technology, primarily for the purpose of demonstration, prototyping and/or basic testing of compatibility between applications. Applications can often be integrated together in a bespoke way to orchestrate data exchanges or workflows and detailed specifications and/or an overall architecture is often not be available. This works well when many parties are offering technology solutions but there is no overall architecture or specification compliance and is best suited for an open innovation or demonstration environment.

A jurisdiction embarking on national or regional digital health programs may make use of these types of environments as the process evolves. A Reference Implementation may be desired early in the process to offer rapid prototyping and demonstration capabilities to help describe the “art of the possible” and to help build a community of practice around digital health in the jurisdiction. As the process evolves, a sandbox environment may be desired which allows the widest possible inclusion of solution vendors and innovators. When the platform has reached a good deal of maturity, a production test system may be offered to trusted parties which mimics the exact live environment in the region – this can be used for precision operations such as conformance testing before applications go live in the production environment.

Annex A. Directorates of the Central 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 6.

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 6 - Common Attributes of Current State Assessments

	Anti-Leprosy Campaign	Health Promotion Bureau	Quarantine Unit	TB and Chest Diseases	National Dengue Control	Anti Malaria 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	

	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
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			
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							

	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
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			
Track the status, delivery, and consumption of consumables/stock/supplies.				X	P	X	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 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		

	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
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			
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	Interchange Standards
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
DMMS	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	HL7, CDA, DICOM, ICD10
eIMMR	Electronic Indoor Morbidity and Mortality Register	National	ICD10
eRHMI	Electronic Reproductive Health Management Information System	National	HL7
Cloud HHIMS	Cloud Based Hospital Health 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.
	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. External Change Request / Issue Process

The information below should be used to suggest edits / changes to Sri Lanka Digital Health Blueprint and its related artifacts. The internal working group will review these changes and integrate them into the primary document after review. It is important that you include the revision number of the document for which the change is proposed as line and section numbers may change. This information can be e-mailed to the tracker

Your Name:	
Your Company/Organisation:	
Document:	[ ] Enterprise Architecture Blueprint (Version 1.0 rev 3613) [ ] Interoperability Plan [ ] Procurement Plan [ ] Other (include name of document)
Version / Revision:	
Submission Date:	
Sections Impacted:	

Your change request should include the section/line number which needs to be changed. Authors of change requests should use ~~strikethrough~~ to indicate text to be removed, and underline for text to be added. For example:

Change Line 3070:

A refresh_token which can be used by the point of service to extend the bearer token ~~beyond its initial expiration~~ once the session has expired which will result in a new series of identity, access and refresh tokens being conveyed to the requestor.

Alternately, you can specify an entire section or bullet to be removed or changed, as an example:

Replace Line 3070 from:

A refresh_token which can be used by the point of service to extend the bearer token beyond its initial expiration

With:

A refresh_token which can be used by the point of service to extend the bearer token once the session has expired which will result in a new series of identity, access and refresh tokens being conveyed to the requestor.

Annex F. Table of Figures