4. Application Architecture

4.1 Current State

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

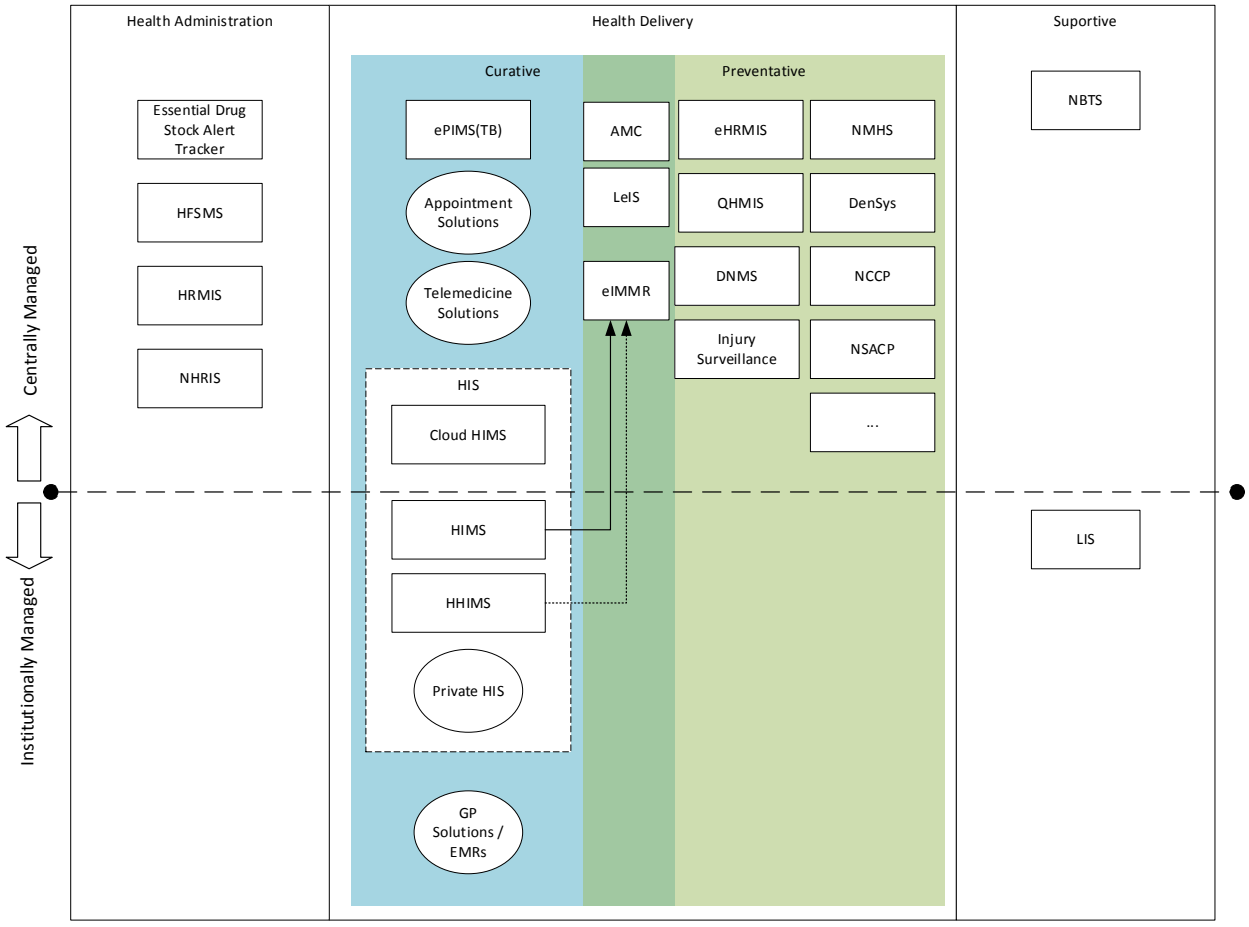

Figure 12 – Current State Conceptual Architecture

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

List of abbreviations:

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

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

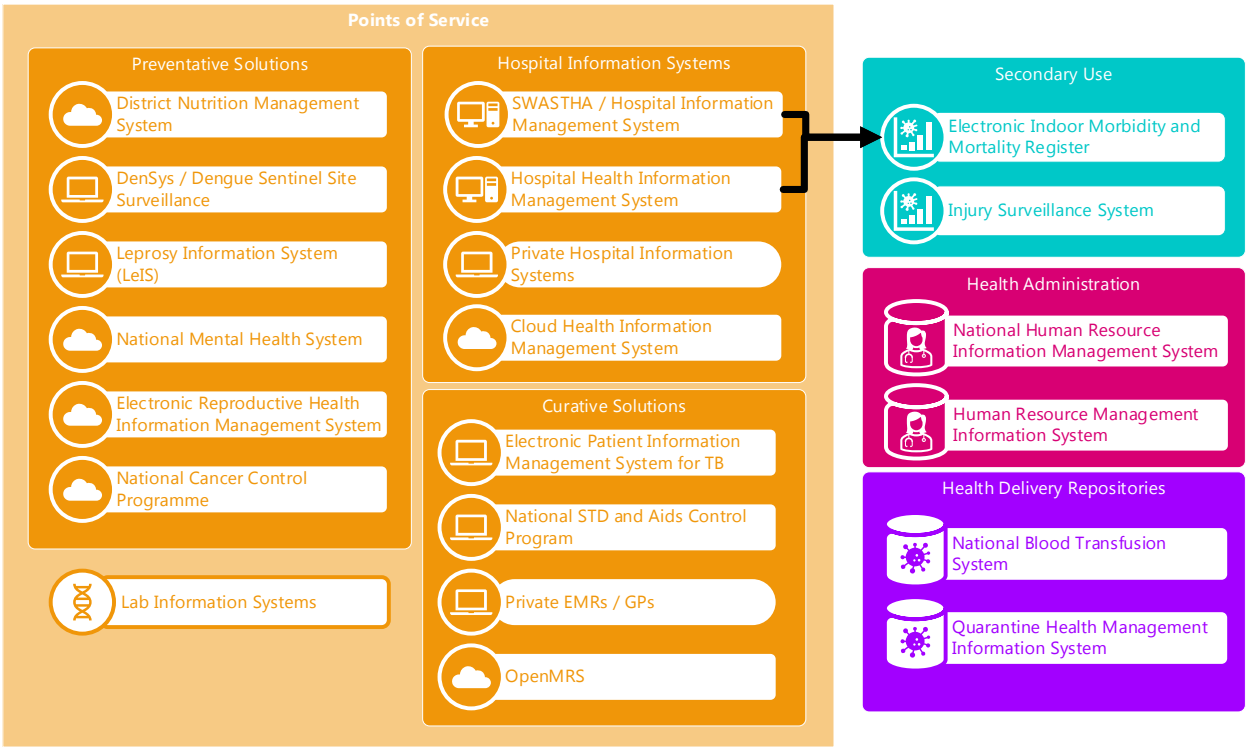

Figure 13 - Current Application Architecture State (Blueprint Nomenclature)

4.2 Proposed Future State

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

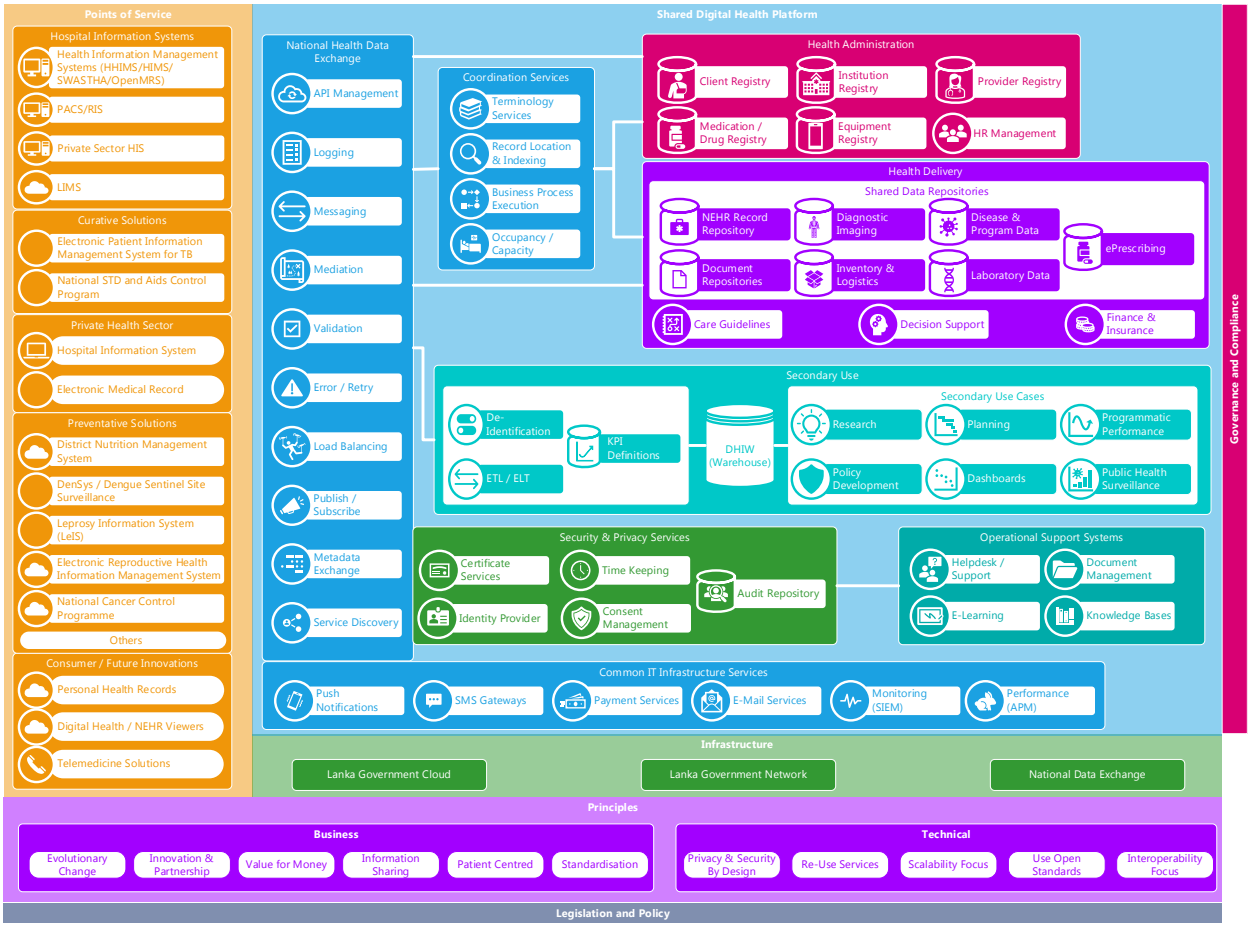

Figure 14- Conceptual Application Architecture

4.2.1.1 Separation of Service Definition from Service Implementation

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

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

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

4.2.1.2 Infrastructure Diagrams

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

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

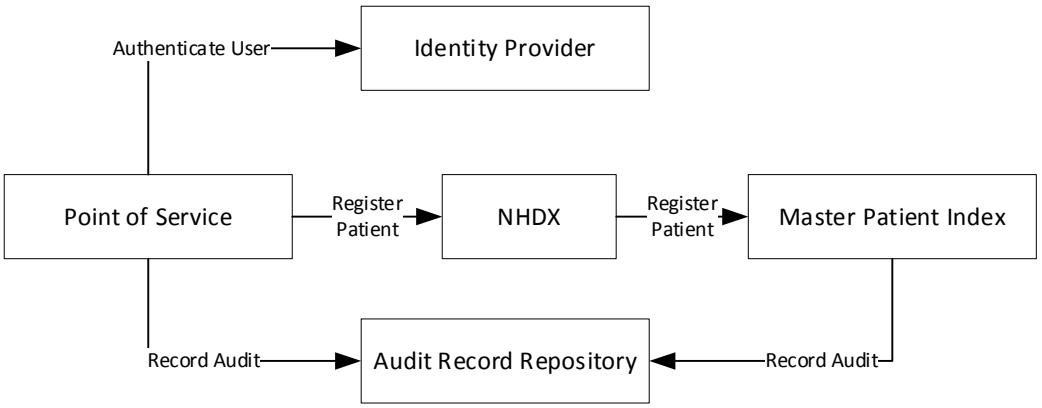

Figure 15- Technical Actor Relationships

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

Figure 16- Simplified Actor Relationship

4.2.2 Points of Service

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

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

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

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

4.2.2.1 Hospital Information Systems (HIS)

There are many Hospital Information Systems in Sri Lanka. All such systems will make extensive use of the DHP, with many relevant use-cases of both retrieving and contributing information to the DHP. For example, the DHP can be used by the HIS systems to:

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

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

4.2.2.2 Curative Sector Solutions

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

4.2.2.3 Preventative Sector Solutions

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

4.2.2.4 NEHR Viewers / Personal Health Records (PHR) Systems

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

4.2.3 Shared Infrastructure

The shared infrastructure domain is described in Figure 17 and specified further in this section.

For reference, the components of the conceptual architecture included in shared infrastructure domain are illustrated in Figure 14.

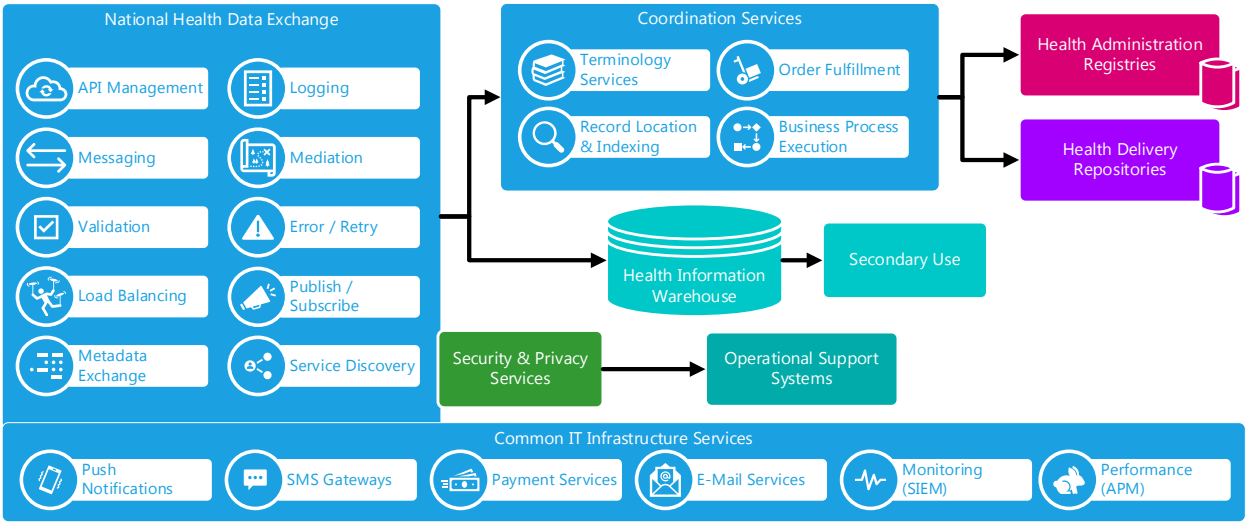

Figure 17- Shared Infrastructure Components

Shared infrastructure domain primarily addresses concerns with:

- Ensuring messages delivered to the DHP are reliably executed, retried, and tracked, ensuring that transactions are not executed twice on retry, relaying errors, etc.
- Services which ensure that the semantic meaning of messages are understood by all digital health services operating within the DHP.
- Communications gateways and common infrastructure for sending notifications to administrators, clinicians and providers including SMS, push notifications and e-Mail gateways.
- Transportation of messages to/from data services including proxying, message relays, etc.
- Service coordination:
    a. Business process execution allowing for complex workflows to occur within the DHP
    b. Terminology resolution, definition, validation, and mapping.
    c. Establishing linkages between orders (request for something), promises (intent to act), and fulfilment (event occurrence) which cross boundaries.
- Error reporting and retry of failed messages
- Enterprise service bus functions such as publish and subscribe management
- Access logging and basic API access control

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

Sri Lanka Telecom (SLT) also provides shared infrastructure services, and several solutions (such as the Suwapetha drug information system) are hosted on the SLT infrastructure. The security

services domain describes a mechanism for node authentication which will permit the interchange of data in a secure manner between these two environments.

4.2.3.1 National Health Data Exchange (NHDX)

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

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

4.2.3.1.1 Messaging Services

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

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

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

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

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

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

4.2.3.1.2 Mediation Services

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

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

4.2.3.1.3 Validation

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

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

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

4.2.3.1.4 Error and Retry

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

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

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

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

4.2.3.1.5 Service Discovery & Metadata Exchange

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

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

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

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

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

4.2.3.1.6 Logging

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

4.2.3.1.7 Load Balancing

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

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

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

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

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

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

4.2.3.1.8 Publish and Subscribe

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

4.2.3.1.9 API Access Control

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

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

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

4.2.3.2 Terminology Services

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

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

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

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

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

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

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

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

4.2.3.3 Record Locator / Index

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

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

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

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

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

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

4.2.3.4 Business Process Execution

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

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

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

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

51. IHE ITI TF Vol1 Cross Enterprise Document Sharing

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

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

4.2.3.5 Common IT Infrastructure Services

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

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

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

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

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

4.2.4 Health Administration

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

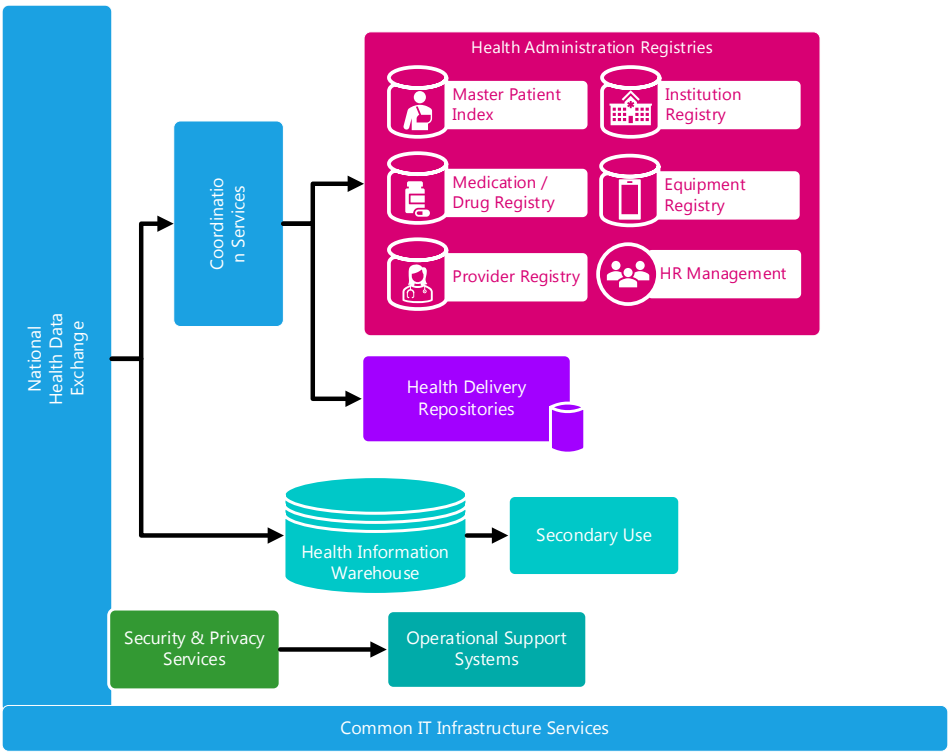

Figure 18- Health Administration Conceptual Components

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

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

4.2.4.1 Client Registry

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

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

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

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

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

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

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

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

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

4.2.4.2 Provider Registry

The distribution of health records across organisations and services necessitates the consistent identification of those persons which are responsible for the delivery of care services. This is the primary role of the provider registry (sometimes called as health provider directory, or health worker registry). Additionally, many health provider registries offer linkage to provider's service delivery capabilities (i.e., dermatology, oncology, or others) which can be used for matching providers with patients in need of those capabilities, while this is not possible currently its inclusion is noted for future development.

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

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

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

- Professional Registration Number and Issuer (college, association, or other)

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

- 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[58], 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 Institution Registry

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

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

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

4.2.4.4 Medication & Device Registry

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

A medications and device registry will be used to track the substances (supplements, vaccines, therapeutics, or other) and medical devices (pacemakers, prosthetics, insulin pumps, etc.)

58. Evaluation of Electronic Health Information Systems (HIS) for the Ministry of Health, Nutrition, and Indigenous Medicine [5] Table 6 - https://arch-lk.health/dmsf/files/3/view
59. OpenHIE Facility Registry Implementation Guide - Google Docs
60. National Digital Health Guidelines and Standards [2] Section 7.3

which can be ordered, delivered, prescribed, and administered within the country.

The primary functions of such a drug registry are:

- Provide consistent identification of drugs and materials beyond simple codes (which merely classify a type of drug, rather than a particular product)
- Provide classification of medications using standardized codes (WHO ATC61, SNOMED CT62, CVX63, RxNORM64)
- Provide detailed information about the form, ingredients, and size/quantity of the medication,
- Provide linkages with types of registered drugs with manufactured products which can be ordered and tracked through cross-organisation logistics workflows,
- Allow for rapid withdrawal of products and lot numbers based on manufacturer guidance.

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

4.2.4.5 Equipment & Supplies Registry

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

The primary functions of the equipment registry are:

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

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

4.2.5 Health Delivery

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

- Admissions and discharges to/from hospitals within Sri Lanka
- Referrals to specialised care providers, or transfers between hospitals
- Diagnoses and treatment of non-communicable and communicable diseases
- Pharmaceutical workflow coordination (prescription, foundry, dispense, administration and status)

61. Anatomical Therapeutic Chemical (ATC) Classification (who.int)
62. Drug or medicament (snomedbrowser.com)
63. IIS | Code Sets | CVX | Vaccines | CDC
64. RxNorm (nih.gov)
65. Medication - FHIR v4.3.0 (hl7.org)
66. Product Recall | GS1
67. Item Data Notification | GS1
68. Device - FHIR v4.3.0 (hl7.org)

- 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

The components within this domain are illustrated in Figure 19.

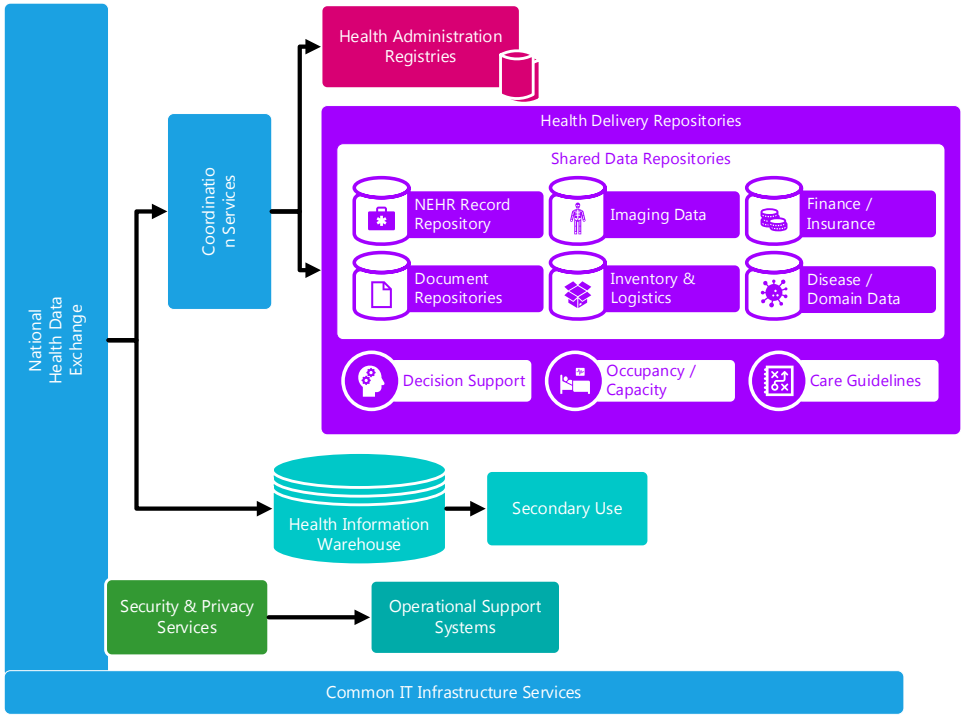

Figure 19- Health Delivery Domain Conceptual Components

- 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 the NEHR Record Repository, Imaging Repositories, Disease and Domain repositories. These repositories require the use of heterogenous data formats based on their domain, so the DHP defines a pattern of multiple repositories (like PDFs, DICOM WSI images, digital pathology systems, and genomics) to facilitate this requirement.
- *Decision Support Services:* Which are used to provide clinical decision support to systems by proposing actions which should occur in order to adhere to a best practices, or relevant clinical protocols.

- *Care Guideline Repositories / Clinical Knowledgebases:* For storing the definition of clinical protocols in machine readable and human readable forms.
- *Inventory and Logistics Services:* The digital capturing, management, and reporting of stock levels, ordering and despatching stock.

4.2.5.1 National Electronic Health Record (NEHR) Repository

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

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

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

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

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

4.2.5.2 Imaging Repositories

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

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

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

69. National Digital Health Guidelines and Standards guide [2] section 7.7
70. Cross-enterprise Document Sharing for Imaging - IHE Wiki
71. Web-based Image Access - IHE Wiki

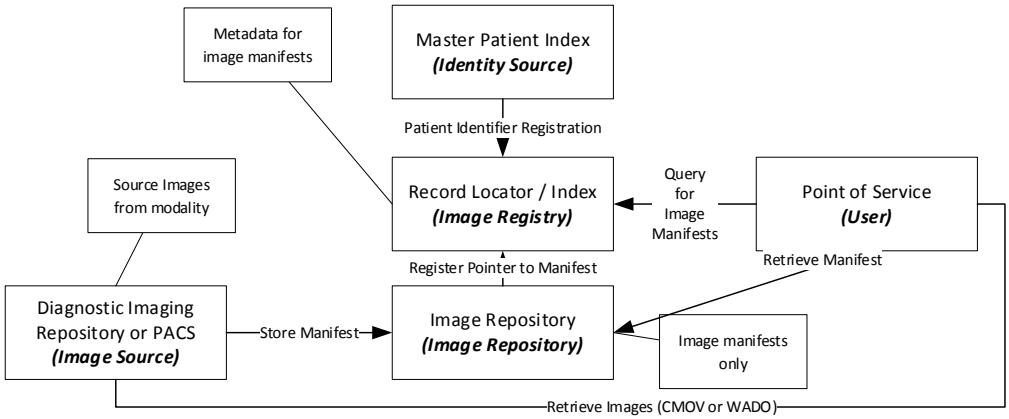

Figure 20- XDS-I Image Exchange in DHP

4.2.5.3 Disease & Program Specific Repositories

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

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

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

4.2.5.4 Clinical Document Repositories

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

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

72. IHE ITI TF XDS.b Vol1

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.

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

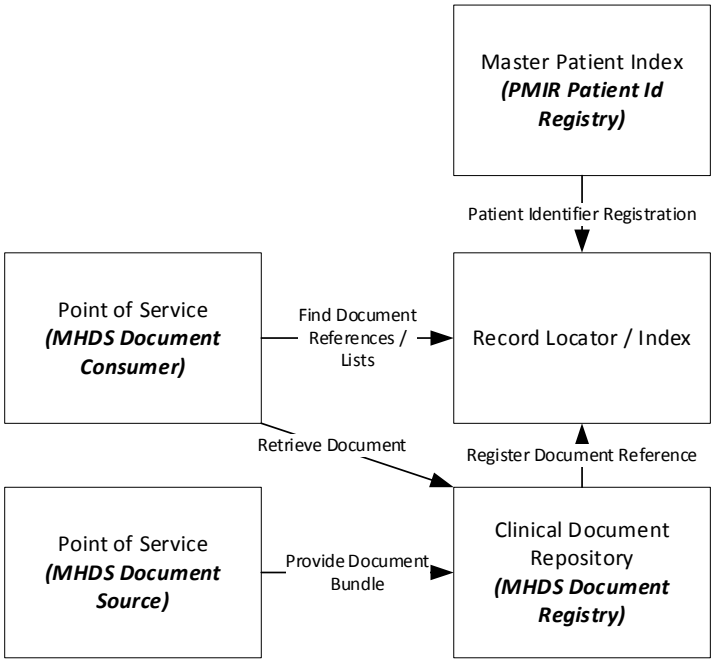

Figure 21- MHD and MHDS in the DHP

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

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

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

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

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

73. HL7 CDA | Lyniate
74. Documents - FHIR v4.3.0 (hl7.org)
75. IHE.ITI.MHD\MHD Home - FHIR v4.0.1
76. IHE.ITI.MHDS\1:50. MHDS Volume 1 - FHIR v4.0.1

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)[77] represent a more widely adopted and mature series of interchanges for logistics and should be implemented as part of logistics and inventory processes in future.

4.2.5.6 Care Guidelines Repository

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

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

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

The contents of this repository will include:

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

4.2.5.7 Clinical Decision Support Services (CDSS)

The storage of care guidelines within the care guideline repository is a first step to the tracking of intelligent health systems. While robust points

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

of service implementations can be expected to directly consume and execute/adhere to these care guidelines, the blueprint proposes the DHP expose necessary services for execution of CDSS rules by all services within the DHP.

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

4.2.6 Secondary Use

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

The primary purpose of secondary use components:

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

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

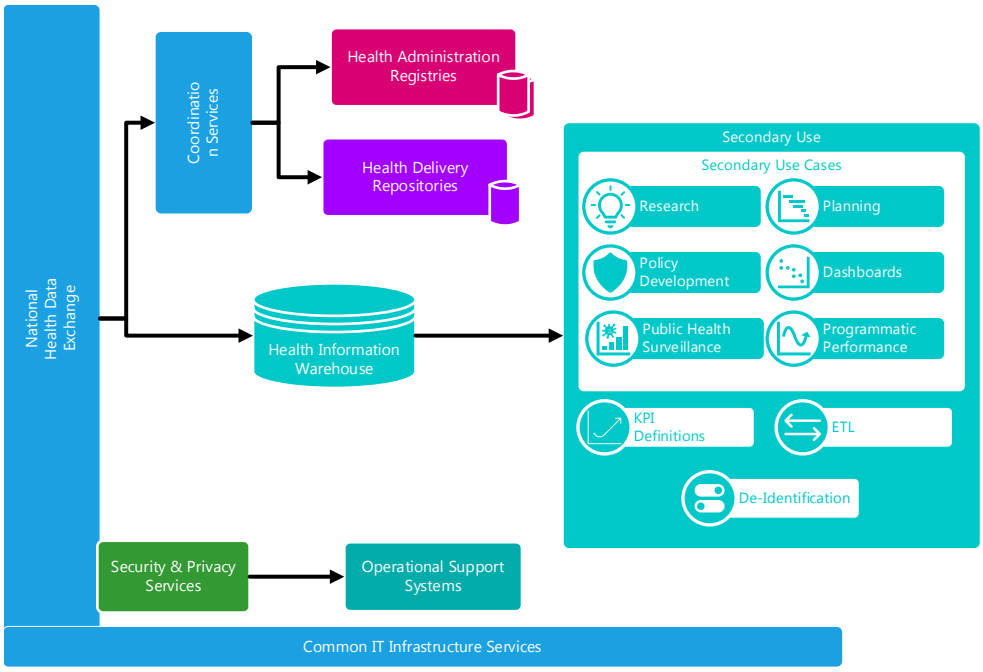

Figure 22- Secondary Use Domain Conceptual Architecture

81. CDS Hooks (cds-hooks.org)

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

- Extraction of data from shared registries and repositories via an ETL process (extract, transform and load) whereby historical events for a reporting period are queried after recordation and the DHIW populated. This pattern is useful for trailing indicators or population of new KPI from historical data.
- Automatic reporting and calculation of secondary use data directly from points of service, registries or repositories using definitions managed by the secondary use system. This pattern is like an ETL process, except each software system computes the data from its own data store and prepares a summary report to the DHIW.
- Automatic capture of secondary use data via the national health data exchange based on subscriptions the DHIW has with the NHDX.
- Manual electronic capture of secondary use data via questionnaires which are populated by administrative users. This pattern is useful for administrative or non-clinical use cases such as functional status of equipment, planned outreach sessions, and others.

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

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

The responsibilities of the DHIW include:

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

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

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

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

4.2.6.1.1 Extract Transform Load (ETL) Services

While the distribution of computable KPI to be completed by software solutions is possible, it is understood that not all software may be capable

82. MeasureReport - FHIR v4.3.0 (hl7.org)
83. QuestionnaireResponse - FHIR v4.3.0 (hl7.org)
84. Data vault modeling - Wikipedia

of performing these tasks. For this reason, the blueprint includes a provision for use of extract, transform and load (ETL)[85] services.

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

4.2.6.1.2 KPI Definitions Repository

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

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

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

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

4.2.6.1.3 Data De-Identification

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

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

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

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

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

4.2.7 Security & Privacy

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

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

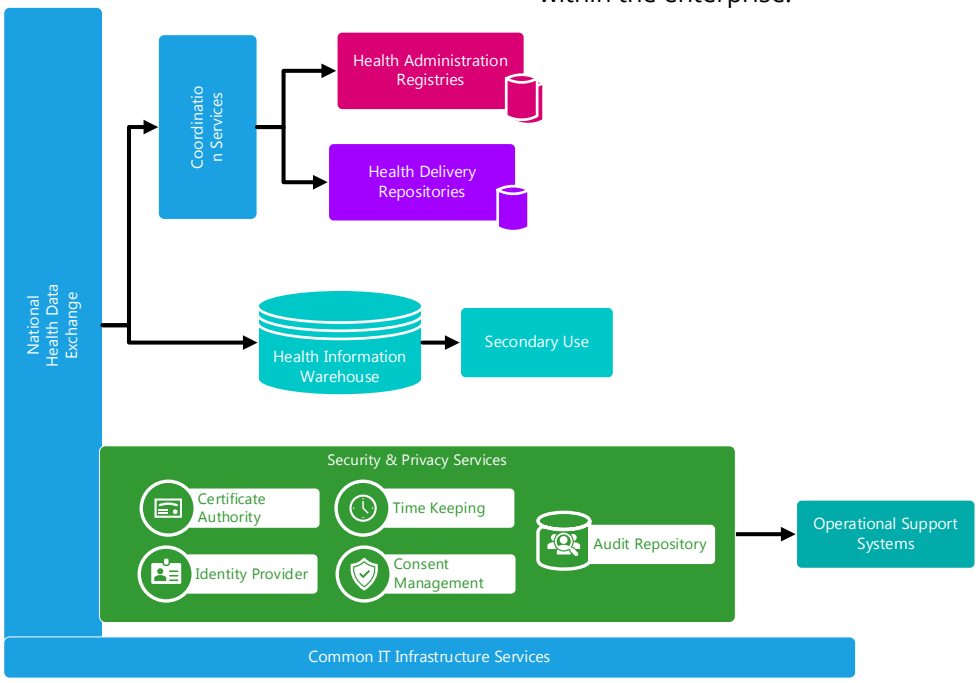

Figure 23- Security & Privacy Domain Conceptual Architecture

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

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

4.2.7.1 Time Keeping / Consistent Time

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

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

91. RFC 1305 - Network Time Protocol (Version 3) Specification, Implementation and Analysis (ietf.org)
92. IHE ITI TF Vol1 - Consistent Time

4.2.7.2 Certificate Services

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

- A Certificate Authority (CA) which is responsible for issuing, revoking, generating, and managing encryption certificates using RSA public/private key architecture[93]
- A key distribution service (KDS) which allows services to obtain public keys for validation of signed data following the JSON Web Key[94] specification. The key distribution service should be publicly available and should use the JSON Web Key Set[95] pattern.

4.2.7.2.1 Security Certificates

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

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

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

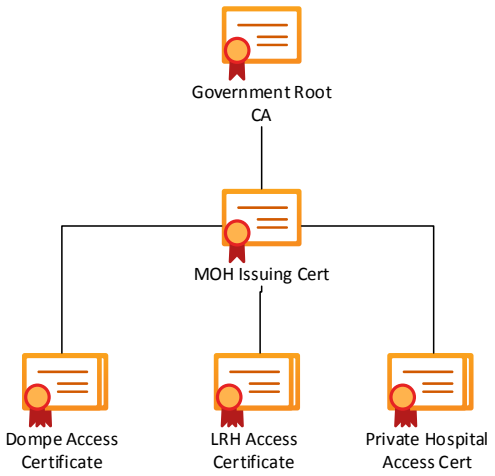

Figure 24- Certificate Chain of Trust

93. RFC 3447 - Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 (ietf.org)
94. RFC 7517 - JSON Web Key (JWK) (ietf.org)
95. JSON Web Key Sets (auth0.com)
96. IHE ITI TF Vol2 – Authenticate Node
97. SMART Health Cards Framework

4.2.7.3 Audit Repository

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

Audit repositories are vital within a health system as they provide a complete list of logical security and data events which occur within the enterprise and allow for investigation and tracking of user activity for compliance and patient privacy audits. A well-supported audit repository within the DHP allows administrators to:

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

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

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

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

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

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

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

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

4.2.7.4 Identity Provider

The digital health platform uses a services-oriented architecture whereby requests will be transmitted between software solutions via API service calls.

98. National Digital Health Guidelines and Standards [2] 6.3.3
99. IHE ITI TF Audit Trail and Node Authentication - Vol1
100. RFC 3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications
101. A.5 Audit Trail Message Format Profile (nema.org)
102. AuditEvent - FHIR v4.3.0 (hl7.org)
103. IHE_ITI_Suppl_RESTful-ATNA

This requires that each API know the identity of the calling application to apply specialised business rules, access controls, or privacy controls.

The DHP will use a bearer token strategy to facilitate the transmission of authentication context between services. The bearer token will be generated and digitally signed (to prevent tampering) from a centralised identity provider using the credentials issued to the PoS using OpenID Connect[104] and OAUTH 2.0[105]. This implementation should be compatible with SMART on FHIR[106] and IHE Internet User Authorization (IUA)[107].

4.2.7.4.1 Application Authentication

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

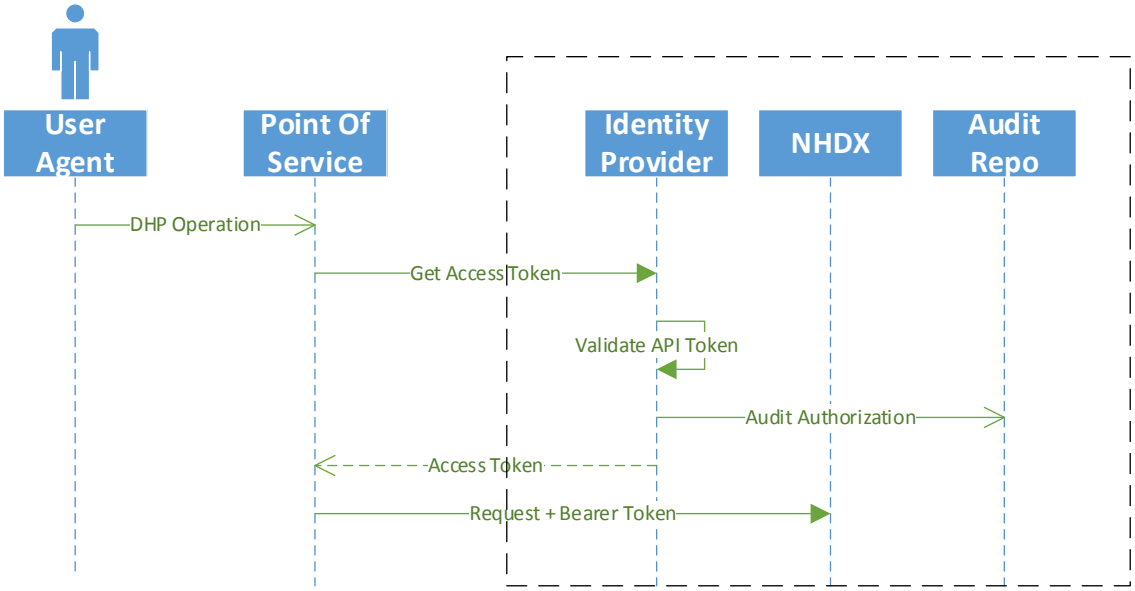

Figure 25- Client Credentials Flow

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

4.2.8 Operational Support

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

104. Specifications | OpenID
105. Map of OAuth 2.0 Specs - OAuth 2.0 Simplified
106. HL7.FHIR.UV.SMART-APP-LAUNCH\Overview - FHIR v4.0.1
107. IUA (ihe.net)

The operational support concerns include:

- Learning Management Systems (LMS) which to provide e-Learning courses to staff, providers, administrators, and other users of the DHP. As the DHP functionality grows, new policies are enacted, or general business processes, and new technologies invented the change management will be an important factor facilitated by the LMS.
- Helpdesk(s) and issue ticketing systems are a key piece of any operational enterprise software solution. It is important to ensure that operators of points of service solutions have a solution where they can raise issues, and follow-up on the status of those tickets.
- Enterprise Knowledgebases & Document management solutions are important for the management and dissemination of policies, circulars, technical documentation, or public documentation whilst maintaining a complete set of version history for documents.

4.3 Evolving the Blueprint

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

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

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

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

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

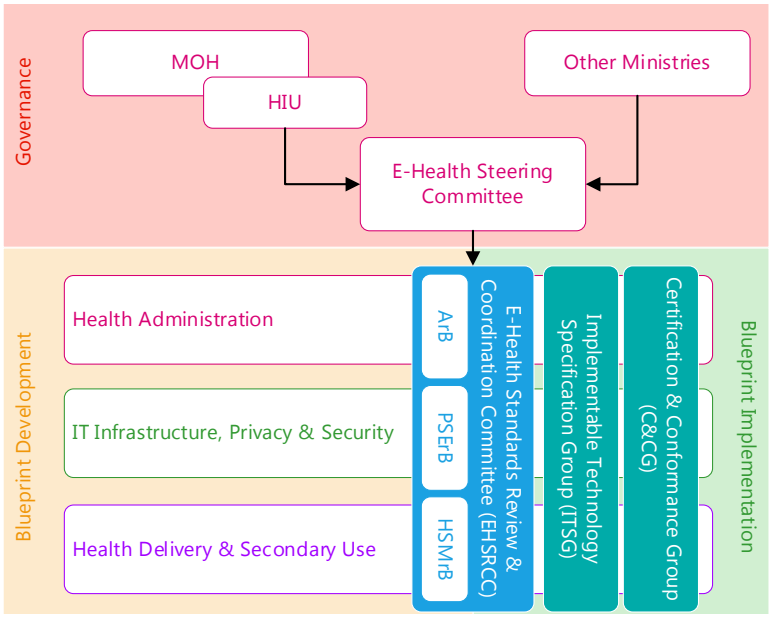

Figure 26- Blueprint Modification Structure

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

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

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

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

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

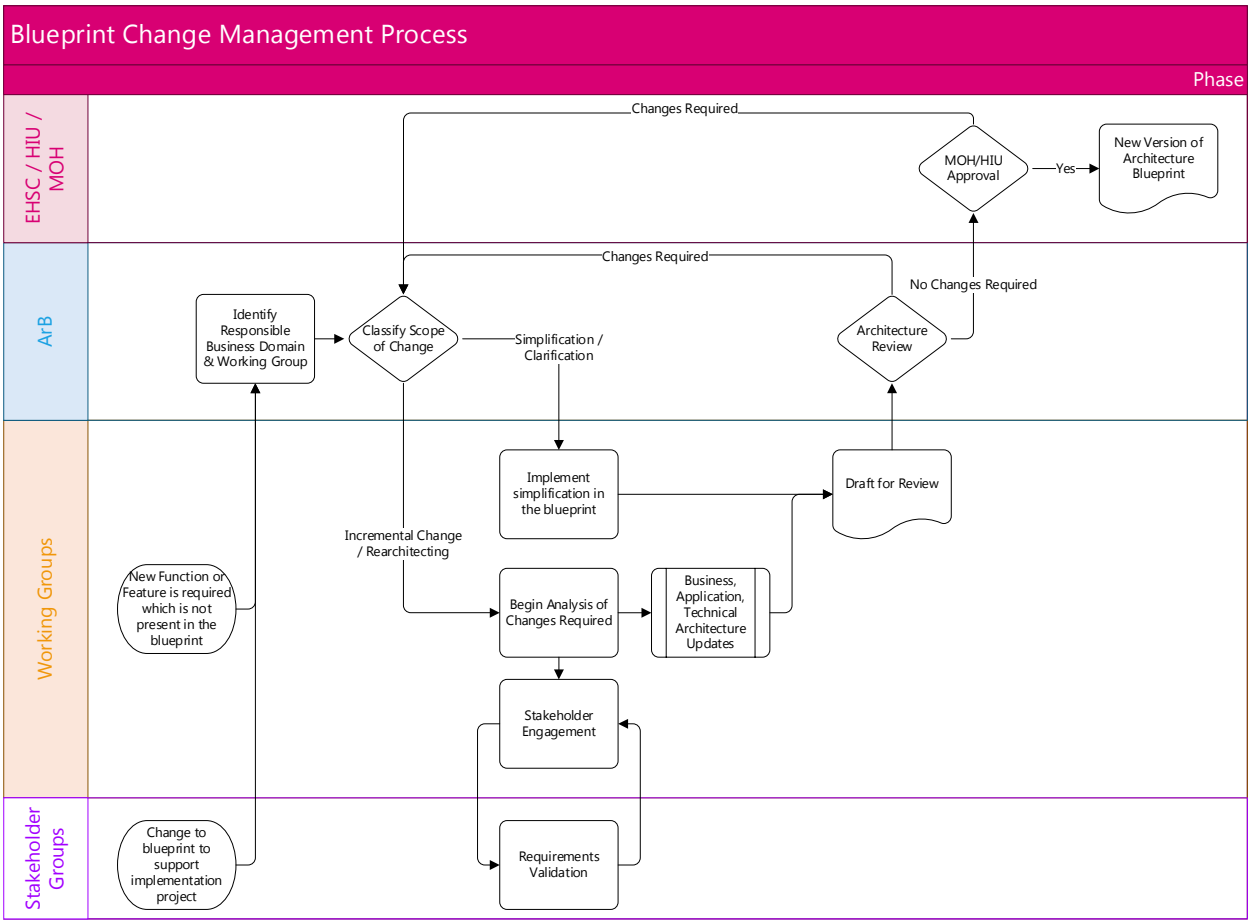

Figure 27 - Blueprint Change Process

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