Copyright Notice

Copyright © Province of British Columbia

All rights reserved.

This material is owned by the Government of British Columbia and protected by copyright law. It may not be reproduced or redistributed without the prior written permission of the Province of British Columbia.

Disclaimer and Limitation of Liabilities

This document and all of the information it contains is provided "as is" without warranty of any kind, whether express or implied.

All implied warranties, including, without limitation, implied warranties of merchantability, fitness for a particular purpose, and non-infringement, are hereby expressly disclaimed.

Under no circumstances will the Government of British Columbia be liable to any person or business entity for any direct, indirect, special, incidental, consequential, or other damages based on any use of this document, including, without limitation, any lost profits, business interruption, or loss of programs or information, even if the Government of British Columbia has been specifically advised of the possibility of such damages.

Document Details

Author: MOH Conformance and Integration Services

Date Created: 2004-08-05

Last Updated: 2020-01-31

Version: 5.1
1.0 Introduction

The Health Information Access Layer (HIAL) provides a standards-based message set for securely exchanging electronic health information with Ministry of Health (the “ministry”) information exchange (HIE) services, including standards, common services and communication services required to integrate applications. The HIAL defines service components, service roles, information model and messaging standards required for the exchange of electronic health record (EHR) data from HIE services.

1.1 Purpose of Document

This document provides an overview of the HIAL architecture and its relationship to the EHR. The material covers the architectural overview for a point of service (POS) connection to the HIAL.

1.2 Intended Audience

The intended audience for this document is technical staff involved in application development and integration of POS systems connecting with ministry HIE services.

1.3 Overview

Delivery of HIE services involves the following major components and features:

Electronic Messages

Patient identification, patient clinical health information and health care provider information is accessed using electronic messages based on HL7 Version 3 and Version 2 standards. The messages are transmitted securely between points of service and the HIAL over health networks. Electronic message contents include a governance header and a payload: the governance header provides information required by the HIAL to enforce security and access policy and the payload contains the relevant HL7 business message(s).
Health Information Access Layer (HIAL)

The HIAL is a web service message-handling infrastructure, providing the “front door” for message-based EHR access. The HIAL is a single consistent interface for POS systems to consume EHR data, providing:

- Security and access policy enforcement;
- Consent and disclosure management;
- Provision of log and audit capability; and
- Message routing to clinical domain repositories

The HIAL is deliberately designed to be message payload agnostic; it uses governance header information to apply security and access policy and does not process message payloads.
2.0 Physical Connectivity

This section discusses the model for physically connecting points of service to EHR services.

Figure 1 below places the components described earlier, in context and provides detail on the structure and interconnection of these components. On-boarding of POS systems involves configuration across many of these components and having this context will assist in understanding of tasks and requirements.

Figure 1 HIAL Architecture

2.1 Protocols

The transport protocol between the POS endpoint and the HIAL is mutually authenticated HTTPS. Mutual authentication requires the POS to both supply and install certificates. These certificates are exchanged as part of the registration process.
3.0 Logical Connectivity

This section discusses the HIAL logical connection model. The model supports flexible connection options and EHR requirements for security, privacy and audit. The model contains entities such as organizations, applications, end-points and points of service that represent real world entities. Logical configuration of a HIAL connection requires definition and registration of each of these entities.

To this point in the document the term “Point of Service” is used generically to refer to the application and system infrastructure where EHR messages originate and where responses are delivered. However, to support varied connectivity approaches the HIAL refines this generic view and separates the following concepts:

- **Endpoint** – a physical web service endpoint where messages are delivered.

- **Point of Service application instance** – the logical destination point for the information contained in the message. In the following material, the term “Point of Service” is frequently used as an abbreviation for the more correct term “Point of Service application instance”.

Separating these concepts supports:

- **Hosting** – where one endpoint supports multiple instances of a single point of service application.

- **Multiple POS applications** – where one endpoint (e.g., broker) supports multiple applications, each independently issuing messages and receiving responses.

- **Reliability** – where multiple end-points support a single point of service providing redundant communication paths to the point of service.
3.1 Entity Descriptions

3.1.1 Organizations

Organizations are business entities that use HIAL services via one or more point of service application instances. That is, a POS executes an interaction on behalf of an organization. An example of an organization is a hosting service provider, hospital, or a medical clinic. Each organization is given a unique organization identifier. The organization identifier is assigned through a registration process.

Key contact roles in the organization:

Privacy Officer – is alerted about privacy events. It is possible for the HIAL to send an email notification to an organization’s designated privacy officer or parent organization when a privacy breach is suspected.

3.1.2 Applications

A software product registered with the HIAL must be authorized to consume domain and registry services. Registration associates the software organization and their application with specific message sets (see below) that are authorized for use by the application.

Individual instances of the application (point of service application instances or application instances) are also registered (see below).

3.1.3 End-points

An Endpoint is a network addressable web service client that communicates directly with the HIAL over a unique TCP/IP address. Integration brokers or hosting sites are examples of end-points. An organization may connect to the HIAL through one or many end-points. Each endpoint has an identifier - a Point of Service endpoint Identifier (POSEID).

An Endpoint must be registered with the HIAL before the HIAL will accept communication from the endpoint. Endpoint registration involves identification of the endpoint (e.g., name, IP address) as well as exchange and installation of certificates to enable mutual authentication. The organization submits a certificate signing request during registration which will be signed by HIAL administration and returned. The organization must also accept and install a HIAL certificate on the web service client machine.
3.1.4 Point of Service Application Instances

A POS Application Instance is an individual instance of a registered application. Each POS application instance is registered against one or more end-points and issues EHR messages and receives responses through that endpoint. Each instance has an identifier, a POSAID. All messages must identify the specific application instance; the endpoint may use the application instance identifier (POSAID) for message routing and delivery.

3.1.5 End-points and POS Configurations

There are several possible configurations of how POS applications can connect to end point instances, which in turn connect to HIAL.

These are illustrated below:

Case 1: POSAID to POSEID

![Diagram: Single POS and Endpoint]

Figure 2 Single POS and Endpoint

In Case 1, where a POS Application Instance (POSAID) is 1-1 with an endpoint instance (POSEID), the application instance uses a single endpoint (unique IP) to connect to the HIAL. Similarly, all other instances of that application use their own dedicated end-points to connect to the HIAL. This case only supports message routing to a single destination with a 1:1 relationship with an IP address and does not easily support configurations where a single IP address supports multiple separate and distinct message streams.
Case 2: Load Balancing/Failover

Figure 3 Single POS, Multiple End-points

In more complex cases, such as when a given application instance uses load balancing, failover, or other distribution techniques, a given application instance can have multiple end-points communicating to the HIAL.

Case 3: Brokered Endpoint

Figure 4 Multiple POS, Single Endpoint

The converse is also possible, such as when multiple application instances go through a brokered endpoint. This configuration supports routing and delivery of multiple message over a single IP address. The endpoint uses the application instance identifier to identify message sources and destinations for routing purposes.

This configuration supports hosting models where a single organization supports individual points of service (e.g., medical practices) or a hosting organization, acting as a broker, supports an aggregation of messages from other independent organizations.
Hosted Solution Configuration Guidance

Software organizations providing a medical practice application (EMR) must implement and operate solutions using an ASP hosting model. Multiple clinics will use a single EMR ASP deployment and it is the EMR ASP system’s responsibility to manage the distinct clinics and clinical users. The EMR systems will register their application in HIAL.

In this case:

- The software organization:
  - which will be registered and assigned a Vendor ID will have the application registered and associated with it.
  - (operating the EMR ASP) is registered in the HIAL as an Organization and assigned an ORG ID and a Realm.
    - which is also responsible for connectivity to the HIAL, is assigned an End Point ID (EID).

- The EMR ASP application instance will be registered as a POS application instance and will be assigned an Application Instance ID (POSAID) associated with the software organization’s End Point.

- The POS will be associated with the software organization’s realm.

- Optionally the HIAL supports the ability to have each of the EMR’s client clinics registered as child organizations under the EMR software organization and assigned their own ORG IDs and Realms.

- This will allow clinic users to be associated with a clinic organization. If clinics are not set up as child organizations, then the clinic users would be registered under the EMR software organization.
4.0 Messages

End-points communicate with the HIAL using industry standard web service SOAP messaging over an HTTP/SSL transport. The structure of a typical SOAP message is shown in the following diagram.

**SOAP Header**

Message SOAP headers contain HIAL governance material including an interaction identifier. The header metadata is validated against a service governance contract and governance validation varies by service (see Governance section below). However, for all messages the following governance identifiers must be present and pass enforced validation.

- Point of Service Endpoint Identifier (POSEID);
- Point of Service Application Instance Identifier (POSAID);
- Organization Identifier;
- Message Identifier;
- Interaction Identifier; and
- Message UTC Creation Date/Time.

**SOAP Body**

The SOAP body contains the relevant domain message. The provincial lab repository (PLIS) uses HL7 version 3 messages. PharmaNet uses HL7 version 2.1 messages provided in the payload as a Base64 encoded string. Message payloads are passed directly to the applicable domain or registry.

*Figure 5 Health Information Exchange Message Structure*
5.0 Interactions

A HIAL transaction refers to an initiating interaction (request message) and all possible response interactions (response messages, failure messages) and implements a specific domain or registry service business function. Every interaction has a unique identifier (interactionID) and every message must contain a valid interactionID.

For HL7 version 3 messages, the HIAL interaction identifier is typically the same as the HL7 interaction for the payload. In BC, these can be localized names rather than Canadian or international interaction names.

The interaction ID specified in the request message is pre-registered in the HIAL as part of configuring a domain or registry service.
6.0 Message Sets

Message Sets are named sets of HIAL interactions. Applications and point of service application instances are assigned specific message sets during the registration process. Points of service application instances must only issue interactions from the set(s) authorized for that POS. This rule is enforced by the HIAL.

A message set can be considered as a role - once created it is easy to assign message sets to any POS as needed. The table below provides fictitious example of message sets, related message interactions and identifiers.

Table 1 Message set example

<table>
<thead>
<tr>
<th>Message Set</th>
<th>Message Interactions</th>
<th>Message Identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMR-PNET</td>
<td>PharmaNet Transaction TDR_00.50</td>
<td>TDR_00.50</td>
</tr>
<tr>
<td></td>
<td>PharmaNet Transaction TRP_00.50</td>
<td>TRP_00.50</td>
</tr>
<tr>
<td></td>
<td>PharmaNet Transaction TRR_00.50</td>
<td>TRR_00.50</td>
</tr>
</tbody>
</table>
7.0 Services

HIAL services are presented as web service end-points. Web service end-points are domain and registry specific and a given domain or registry may support several end-points that apply different governance rules.

The WSDL and XSD files required to access the web service end-points are included in this package. The service URL’s network address is different for each of the development and test, conformance, training, and production environments. The service URL’s network address is provided during the on-boarding process.
8.0 Governance

The message sender (the “client”) must provide complete and accurate information in the SOAP header to support message governance.

When the HIAL receives an interaction request, it applies a set of governance rules (access policies) to the message header before passing the message to the domain or registry for business processing. The data is in XML format and provides the HIAL with the information necessary to apply security, authorization, routing and logging policies to the message. Response messages also contain governance information which may be used by the endpoint or point of service application for response routing or other purposes.

Different HIAL services require different governance header information.
Governance Types

The HIAL supports the following governance types (called ‘aspects’):

- **Common** - The common header is present on all requests to the HIAL and contains governance information that includes message interaction codes, a unique message identifier, message timestamps, and etc.

- **System** - The system header is required on all requests to the HIAL and contains information for HIAL authorization of the sending POS application instance, sending organization, and sending application.

- **User** - The user header identifies the user who has invoked the request and contains information to enable HIAL user authentication for the service request. HIAL users are assigned a provincial “Role” that determines the user’s permissions to use specific HIAL message interaction codes.

- **Client** - The client header is used to identify the client associated with a request and to validate the client against the Provincial Client Registry Composite View. It contains information to enable HIAL verification and logging of the person who is the subject of the message. Typically, the subject’s Personal Health Number (PHN) is provided in this part of the SOAP message, however the use of a Medical Record Number (MRN) is also supported.

- **Provider** - The provider header is used to identify a set of providers with a request and contains information enabling HIAL verification and logging of the health provider who authorized and accepts professional accountability for the interaction. The provider can be different from the user, who may be (and often is) working under the direction of the accountable provider.

- **Disclosure** - The disclosure header is used whenever a user requests patient information that is protected by a Disclosure Directive. It supports management of patient Consent Directives at the point of service.

- **Distribution** – The distribution header is used to identify the set of recipients requesting notification and delivery of events such as delivery of lab results or HIAL alerts.
8.1 Enforced and Reported Aspects

In the context of a particular service request type (e.g., a lab get), the aspect associated with a governance header may be either “enforced” or “reported”. In both cases, the aspect is verified against a source of truth, for example the Client Registry for the client aspect.

If an enforced aspect fails validation, a SOAP fault with an embedded error message is returned to the requesting POS and the service request is not passed on to the domain or registry.

Provided mandatory header fields are included in the header, if a reported aspect fails validation, the request is still executed - the service request is passed on to the domain or registry. However, the failure of the governance step may affect the outcome or may result in warnings being returned to the sender in the response message.

Which aspects are enforced, and which are reported depends upon the governance defined for a particular service. While some aspects are always enforced, and some are always reported, there are aspects that are enforced for some services and reported for others. For example, the:

- **system aspect** (associated with the system governance header) is always enforced;
- **distribution aspect** (associated with the distribution list header) is always reported; and
- **client aspect** (associated with the client header) is enforced for a lab query service reported for a PharmaNet service and not required for a client or provider registry service.

The HIAL executes enforced aspects in a particular sequence with more specific aspects depending upon the prior validation of more general ones. For example, the user aspect depends upon the validation of the system aspect. The first enforced aspect to fail will result in the immediate return of a SOAP fault to the requesting POS, with an embedded error message from the aspect that failed. Should all enforced aspects be valid the reported aspects are executed. Each reported aspect failure results in the inclusion of an aspect error message in the information passed to the service endpoint. This can result in multiple reported aspect error messages in the request passed to the service endpoint.
For example: for the lab query (LabGet) service (POLB_IN354000CA) the enforced aspects are executed in the following order:

- Common;
- System;
- User;
- Client; and
- Disclosure.

There are no reported aspects for a lab query.

A response returned from the HIE service (a domain or registry) may be either positive or negative. As the HIAL is payload agnostic the reader should consult the domain or registry specific conformance document for details on the payload responses that may be returned.

### 8.2 Timeouts

If for some reason the HIE service (e.g., PharmaNet or PLIS) does not return a response in an acceptable time, the HIAL returns a SOAP fault to the POS system with a timeout error message.
9.0 Identifiers

Various application, facility, endpoint (collectively “system”) and organization identifiers are required in payload messages and in the HIAL governance headers. They are used to identify:

- **POS users** – the person at the point of service who requests (perhaps indirectly) an EHR service.
- **Providers** – the provider who is accountable for the EHR service request as well as the provider(s) who participated in the health event.
- **Subjects** – the client who is receiving care or health services. Typically, this client is identified by their Provincial Health Number (PHN) and corroborating demographics such as family name, date of birth and gender.
- **EHR components** – applications, end-points, points of service, messages and interactions.

For messages sent to the HIAL the situation is complex. HIAL messages require governance headers to contain various pieces of system information (indicated by the blue arrow). The HL7 V3 payload also contains conceptually similar but not identical information.

The following diagram provides a general outline:

![Diagram of System and Organization Identifiers](image)

*Figure 6 System and Organization Identifiers*

In several cases, the same identifier is required in both the message header and in the message payload. This can be a conformance requirement.

The use and application of identifiers is a complex topic, in part because of different terminologies between domains.
10.0 Security Models

10.1 Users and Realms

![Realm Logical Model](image)

*Figure 7 Realm Logical Model*

**User**

A user is the person currently operating the point of service application instance when an interaction request is sent to the HIAL. The user is not necessarily the same as the provider who is accountable for the interaction and is identified separately. For example, the user may be a medical office administrator (MOA) using the point of service on behalf of a physician who is the responsible provider.

The user has a user identifier (userID) that uniquely identifies them to the point of service application. The HIAL also requires registration of user identifiers.

**Authentication realm**

An authentication realm serves two purposes:

- It provides a unique namespace for user identities (userIDs). The combination of userID / authentication realm must be unique within the HIAL; and

- It defines an accountable source for authenticated identity. The owner of the realm provides a guarantee the userID contained in messages has been authenticated according to provincial privacy and security standards.

During logical configuration, authentication realm(s) are associated with specific point of service application instances. Only users from within the configured realm(s) may issue transactions from the registered application instance.
10.2 Roles and Resources

Each user registered in the HIAL is assigned one or more provincial Roles. Roles are named sets of protected HIAL resources such as message interactions. The assignment of a role to a user enables use of the (associated) resources.

Provincial roles are pre-defined by the Ministry.

HIAL user registration requires assignment to an appropriate provincial Role. The provincial Role must map to an appropriate point of service role. For example, a point of service office administrator role cannot be assigned a provincial Prescriber role.
11.0 Disclosure Directives (Access Words)

Disclosure Directives for patients (clients) are maintained in the Disclosure Directives Registry.

A Disclosure Directive is an access restriction a patient places on his or her personal electronic health information in the Provincial Laboratory Information Solution (PLIS).

Once a Disclosure Directive has been placed on a client’s information, access to client information via messages (e.g., a query request) is prevented by the HIAL unless the Disclosure Directive is explicitly overridden. The override is done through the use of a Disclosure Header accompanying the request message.

There are two types of disclosure overrides:

- **An override with-consent:** requires a patient to provide their access word which must be encrypted and inserted into the disclosure header of the request message.

- **An override without-consent:** is used in an emergency situation when the user does not have the patient’s access word.
  - The user issuing the request is required to provide an explanation of why the override without consent is necessary.
  - An explanation is inserted into the disclosure header of the request message.
  - Each override without consent results in a notification to the privacy officer of the organization the requestor is acting on behalf of.
12.0 Registration

Use of HIAL services requires registration of various components including:

- Organization information;
- Organization contact information;
- Application;
- Endpoint;
- Point of Service; and
- Users.