BRITISH COLUMBIA
Ministry of Health

British Columbia
Professional and Software Conformance Standards

Electronic Health Information Exchange

Volume 1: Overview & Conformance Processes

Version 3.2   2021-02-26

Security Classification: Low Sensitivity

Copyright Notice

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:	2011-03-04
Last Updated:	2021-02-26
Version:	3.2

Table of Contents

1.0 Introduction

Organizations developing interfaces to health information exchange (HIE) services offered by the Ministry of Health (the “ministry”) must meet the British Columbia Professional and Software Conformance Standards (the “conformance standards”) which the ministry publishes.

The ministry’s Conformance and Integration Services (CIS) will facilitate the registration, connection, conformance testing, and certification processes required for applications to connect to the ministry HIE services.

1.1 Key to Document Terminology

The conformance standards in this volume use a consistent language convention:

- Standards or rules using the words “must”, “will”, “minimum”, or “mandatory” are a compulsory function or requirement. Conformance testing, service on-boarding activities and/ or application testing will confirm that this standard is correctly implemented.

- When the word “optional” is used, it refers to recommended functions or requirements. If implemented, conformance testing, service on-boarding activities and/ or application testing will confirm that this standard is correctly implemented.

- Acronyms and abbreviations are used for repetitions of some system and organization names. The first time an acronym or abbreviation appears in the document it is accompanied by the full name.

- Each defined term, acronym and abbreviation that is included in the glossary is italicized in the conformance standards the first time it appears in the volume. A Glossary of Terms is provided in a separate volume of the conformance standards.

1.2 Ministry Conformance and Integration Services (CIS) Support Team

The Ministry’s Conformance and Integration Services (CIS) Support Team is the point of contact for all questions related to the Ministry’s conformance process, standards, set-up and testing:

- HLTH.CISSupport@gov.bc.ca

1.3 Audience

This volume is intended primarily for software vendors and health organizations developing an interface to HIE service offerings by the ministry. Others with an interest may include health care providers and others who access and exchange health information from a ministry or provincial data repository, ministry information owners, conformance evaluation teams and audit teams.

2.0 Ministry Health Information Exchange (HIE) Services

This section introduces the ministry's HIE services which can be integrated with POS applications.

2.1 Client Registry (CR)

The Client Registry (CR) is the authoritative registry of health care client demographic information in British Columbia including:

- personal health number (PHN),
- health authority source system identifiers (e.g., medical record number),
- name,
- date of birth,
- date of death (if applicable),
- gender,
- address, and
- telephone number.

An integrated POS application can link an individual's clinical records (e.g., lab results) based on the patient's PHN and source system identifiers from integrated systems across the province.

Authorized users with a POS application integrated with the CR can:

- search for and capture patient identity information to support safe health care service delivery;
- store client demographics from the CR in the POS application;
- update client demographic information in the CR; and
- create PHNs for patients.

Note: Every recipient of BC health care service must have a PHN.

2.2 PharmaNet

PharmaNet is the provincial drug information and claims processing system that links all community pharmacies and contains every prescription dispensed by community pharmacies in British Columbia.

Authorized users (e.g., pharmacists and other health professionals) with a POS application integrated with PharmaNet can:

- submit prescription, dispense and claim information;
- access patient medication histories and store them in their local application;
- update patient medication histories with over-the-counter medications, dispensed samples, clinical conditions and adverse drug reactions;
- generate drug monographs for professional information and patient counselling;
- perform drug use evaluations to identify possible drug interactions;
- monitor patient medication adherence by verifying the status of a prescription; and
- identify and warn patients about potentially harmful medication interactions, unintended duplications, and risks from the misuse of prescription drugs.

2.3 Provider and Location Registry (PLR)

The Provider and Location Registry (PLR) is the authoritative registry of British Columbia health care providers' demographic and professional information (e.g., name, identifiers, demographics, expertise, contact, licensing status, and work location) which can be used to maintain internal provider directories within the health sector.

The PLR supports activities such as patient referrals and informal consultations between care providers.

Authorized users with a POS application integrated with the PLR can:

- search for provider demographic and professional information and store the results in their local application;
- receive real time distributions of updated provider information to store in local directories; and
- update a provider's work location information in the PLR.

2.4 Provincial Laboratory Information Solution (PLIS)

The Provincial Laboratory Information Solution (PLIS) contains comprehensive diagnostic laboratory test results from private and public laboratories across British Columbia; and allows authorized care providers to access their patients' historical and recently published lab test results including tests ordered by other health care providers.

Access to comprehensive lab results is important for care providers to make timely and appropriate clinical decisions; and reduces patient inconvenience by preventing the unnecessary duplication of lab tests.

Authorized users with a POS application integrated with the PLIS can:

- view a summary of all lab results within a specified period for a patient;
- select lab results reports to retrieve; and
- view and store the lab results data in the local software for other clinical decision support purposes (e.g., trending, graphing).

NOTE: Integration to PLIS is currently on hold until further notice.

3.0 Ministry HIE Transport Protocols

The ministry provides message-based access to the HIE services to various points of service including pharmacies, medical practices, and health authority facilities. These messages are standardized, secure and authenticated.

The HIE services use the following connection methods to exchange health care information between a point of service (POS) and ministry domain system:

- Health Registries Broker
- HNSecure
- PharmaNet Application Program Interface (API)

HNSecure is ministry-provided software and infrastructure used to securely exchange data over the Internet or other untrusted network. Community pharmacies currently use HNSecure or a PharmaNet API over the provincial pharmacy network to access the PharmaNet system.

4.0 Forms & Agreements

This section describes the agreements used to establish terms and conditions for integrating with ministry HIE services. The applicability of the agreements will depend on the organization's type of system and desired HIE access.

4.1 Vendors

Organizations developing interfaces to Ministry HIE systems must submit all required forms and agreements (which are available at):

- https://www2.gov.bc.ca/gov/content/health/practitioner-professional-resources/software/forms

4.2 Connected Parties (Users and Organizations)

Agreements are required for user/organization access to be granted to ministry HIE systems:

- Site Registration and User Agreements – PharmaNet
- Practitioner Systems Access Agreements (for EMRs) – All domains
- Information Sharing Agreements (for Health Authorities) – CR, PLR, PLIS

For further details, contact CIS Support Team.

5.0 Conformance Standards Overview

The conformance standards are the central reference for organizations wanting to integrate POS applications with ministry HIE services. Organizations developing interfaces to the ministry's HIE services must comply with the conformance standards.

Integration with ministry systems allows users to exchange important demographic and clinical information with other health care professionals in support of efficient and safe patient care.

The conformance standards contain multiple volumes and must be reviewed as a complete set. The set includes common volumes that apply to all organizations, business rules, application rules and technical message specifications for each domain.

The Ministry’s Conformance Standards are available for download from the provincial website at:

- https://www2.gov.bc.ca/gov/content/health/practitioner-professional-resources/software/conformance-standards

5.1 Common Volumes

The following common volumes apply to all organizations:

Volume 1: Overview and Integration Processes

Provides an overview of the exchange of electronic health information with ministry systems. It outlines the content of the conformance volume set and explains the processes and requirements for organizations to access ministry HIE services; including the conformance evaluation process, roles and responsibilities, organization requirements for registration, legal agreements, network and connectivity, and ongoing system management.

Volume 2: Information Privacy and Security

Outlines the information privacy and security controls required to access ministry HIE services.

Volume 3A: Business Rules - General

Defines the business and training rules for POS users who access ministry HIE services. The general business rules apply to all integrations.

Volume 4A: Application Enforced Rules - General

Defines the application rules that must be enforced by POS systems when accessing ministry HIE services. The general application enforced rules apply to all domain integrations.

Glossary of Terms

The glossary defines the terms and acronyms used throughout the conformance standards.

5.2 Domain Specific Volumes

Volume 3: Business Rules

Defines the business and training rules for POS users who access ministry HIE services. There is a volume of business rules for each ministry domain.

- Volume 3B: Business Rules – Client Registry
- Volume 3C: Business Rules – PharmaNet
- Volume 3D: Business Rules – Provider and Location Registry
- Volume 3E: Business Rules – PLIS

Volume 4: Application Enforced Rules and Technical Message Specifications

Defines the application rules that must be enforced by POS systems when accessing ministry HIE services. There is a volume of application enforced rules and technical messages specifications for each ministry domain.

- Volume 4B: Application Enforced Rules – Client Registry
- Volume 4C: Application Enforced Rules – PharmaNet
- Volume 4D: Application Enforced Rules – Provider and Location Registry
- Volume 4E: Application Enforced Rules – PLIS

The following identifies the required conformance standards volumes applicable to each of the ministry domains:

Table 1 Conformance Standards Volume Set

Domains	**Required Conformance Standards Volumes**											
	1	**2**	**3A**	**3B**	**3C**	**3D**	**3E**	**4A**	**4B**	**4C**	**4D**	**4E**
Client Registry	✓	✓	✓	✓				✓	✓			
PharmaNet	✓	✓	✓		✓			✓		✓		
PLR	✓	✓	✓			✓		✓			✓	
PLIS	✓	✓	✓				✓	✓				✓

Note: In addition, select the appropriate transport protocol (e.g., Volume 5B HNSecure).

5.3 Transport Protocol Volumes

Volume 5: Transport Protocol

Provides an overview of the technical mechanisms by which POS systems connect to ministry HIE services. Each protocol has its own set of standards and message specifications.

- **Volume 5B: HNSecure** – HNSecure (inclusive of HNClient, HNServer/HNGate, and HNGard) performs encryption/decryption, authentication and message routing services for organizations to securely exchange electronic health information via the Internet.

- **Volume 5C: API Gateway** – currently under development. Please email: HLTH.CISSupport@gov.bc.ca if you are interested to access the API Gateway sandbox.

Note: Other transport methods (e.g., Health Registries Broker, PharmaNet API) may be available. Please contact the CIS Support to discuss.

5.4 Changes to the Conformance Standards

The conformance standards are:

- updated and published as needed to support changes in legislation, policy, best practices and services included in the HIE services;

- developed and published as a set of related volumes with a common release date/version; and

- contain only the rules for interfacing with ministry HIE services in British Columbia.

- published on the ministry website.

Organizations can sign-up to receive update notifications by emailing:

- HLTH.CISSupport@gov.bc.ca

6.0 Integration Processes

The following table identifies the primary participants and a high-level overview of their responsibilities throughout the integration and conformance processes:

Note: Please see the subsequent sections for more details regarding the integration process.

Table 2 Roles and Responsibilities

Roles	Responsibilities
Software Organizations (e.g., vendors, health authorities)	• Conduct a self-assessment: a self-administered conformance readiness assessment to validate developed functionality prior to requesting a conformance test through the ministry; • Contact the CIS Support Team to establish network connectivity; • Demonstrate system conformance to the conformance standards through conformance evaluation; • Download the conformance standards package; • Establish secure connection to ministry environments; • Configure security requirements, such as user IDs, and server certificates for environments where they are required; • Register for a basic BCeID to gain access to ministry-shared documents, particularly to the API Gateway resources; • Incorporate ministry test data into POS application prior to the evaluation; • Participate in a vendor discovery session to review integration objectives and timelines with the ministry; • Provide POS user support and training of certified application to clients; • Provide client support for user registration; • Review the requirements for connecting to the ministry environments; • Review the conformance standards applicable to your integration goal to understand the requirements; and • Submit all required forms and agreements.

Roles	Responsibilities
Ministry Conformance and Integration Services (CIS) Team	• Coordinate and oversee the conformance evaluation sessions; • Coordinate/facilitate network connectivity; • Coordinate/facilitate connectivity to ministry environments; • Issue conformance certification; • Maintain a registry of certified products; • Prepare the conformance evaluation report; • Provide test cases and test data required for development, conformance evaluation and training needs; • Publish and maintain the conformance standards and education material; and • Receive and facilitate responses to software organizations' questions and issues.
Ministry Domain Evaluation Team(s)	• Evaluate each tested requirement (i.e., pass or fail); • Prepare test cases/data; • Sign/approve conformance test results; and • Validate transactions against applicable test cases and expected results.

6.1 Apply for Integration Services

The ministry assists software organizations interested in integrating with HIE services.

Software organizations must:

- understand the integration requirements by reviewing the integration options, conformance standards, and legal agreement;
- complete and submit a ‘Request for Integration Services’ form to the CIS Support Team.

The ministry will host discovery sessions to:

- ensure the organization’s integration plans align with the ministry business strategy;
- verify understanding of the requirements;
- identify any constraining factors;
- determine the appropriate integration approach; and
- reach a consensus view on whether the time is right to proceed with the integration plan.

6.2 Register for Ministry System Access

All software organizations developing systems for integration with ministry HIE services must register for access to the required environments.

6.2.1 Ministry Service Access Prerequisites

6.2.1.1 Software Organizations

To develop, implement and support software at POS locations that access and exchange data with ministry HIE services, software organizations must:

- adhere to privacy and security obligations (Vol. 2);
- develop software that implements the application enforced rules (Vol. 4);
- ensure users comply with the general and domain specific business rules (Vol. 3);
- follow the processes outlined in this document;
- implement the technical mechanisms to connect to ministry systems as provided in the transport documentation (Vol. 5);
- initiate and complete the conformance process; and
- sign a Vendor Participation Agreement prior to environment access.

6.2.1.2 Point of Service Users

POS software users may only access ministry HIE services using software that has been certified by the ministry as compliant with its conformance standards. A software organization must have their software evaluated through the ministry conformance testing process to receive this certification.

User authentication is managed within the POS software and no additional login is required to access the ministry's HIE services. However, POS users need to be assigned an appropriate role with associated permissions based on their clinical or administrative scope of practice.

To access ministry HIE services, POS organizations and users must:

- follow the registration processes and adhere to the business rules (Vol. 3);
- receive appropriate training; and
- sign a data access agreement.

6.2.2 Environment Access Prerequisites

6.2.2.1 Sandbox Environment Access

The sandbox environment is available for software organizations to complete integration development.

Prior to access being granted to the sandbox environment, software organizations must:

- review all conformance standards and associated message specifications;
- subscribe to vendor notifications to receive changes to the conformance standards;
- understand and commit to all requirements for full integration with ministry systems;
- complete and submit the Request for Integration Services (HLTH 4637) form;
- agree to appropriate sandbox environment usage;
- sign an appropriate vendor participation agreement;
- configure the POS system for connectivity to the environment.

6.2.2.2 Conformance Environment Access

The conformance environment is used by software organizations to demonstrate compliance to the conformance standards.

Prior to access being granted to the conformance environment, software organizations must:

- agree to appropriate conformance environment usage;
- complete and submit a Conformance Initiation Notice (HLTH 4636) to request a formal conformance test;
- configure the POS system for connectivity to the environment; and
- conduct a self-test to validate compliance to the conformance standards.

Note: A self-test must be conducted in the conformance environment to confirm the ability to pass all rules as specified in the conformance standards prior to requesting a formal ministry conformance test.

6.2.2.3 Training and Production Environment Access

The training environment is used to conduct end user training exercises; and can be accessed by end users on an ongoing basis to refresh understanding of and practice using ministry HIE services.

Prior to gaining access to either the training or production environments, software organizations must:

- configure the POS system for connectivity to the environments;
- confirm vendor registration information and provide a privacy contact;
- receive certification from the ministry; and
- understand and use the ministry’s user/vendor support model.

6.2.3 Software Organization Registration

The CIS Support Team will provide guidance on the software organization’s integration and registration for access to the ministry’s sandbox, training, conformance and production environments. Registration to use any of the ministry’s secure networks requires a variety of configuration information.

Software organizations must register for services to start the integration process. The CIS Support Team will be the point of contact for each of the items described in this section.

The applicability of the registration forms will depend on the organization’s type of system and current and desired HIE service access.

6.2.3.1 HNSecure Registration

HNSecure is software developed by the ministry for securely exchanging electronic health information via the Internet. HNSecure, inclusive of HNClient, HNServer/HNGate, HNGard, performs encryption/decryption, authentication and message routing services.

Use of HNSecure by POS applications requires conformant software and Network Facility registration with the ministry. Detailed instructions are provided in Volume 5B: Transport Protocol – HNSecure.

6.2.3.2 Health Registries Broker

Contact the CIS Support Team for information on connecting to the Health Registries.

6.2.4 POS User Registration

The user registration process to access systems in a production environment varies depending on the POS.

6.2.4.1 Health Authority

The registration of health authority users accessing the ministry HIE services follows a decentralized model. Each health authority is responsible for the management of their users and access to ministry systems (e.g., approvals, reviews, breach management, training).

6.2.4.2 Medical Practice

For PharmaNet, medical practices must initiate a formal application process with Health Insurance BC (HIBC) to register its clinic and all users. User access requires technical configuration changes to be implemented by both the POS software provider and the ministry.

The software organization providing the medical practice EMR application may want to prompt the medical practice to register to expedite the process.

Each non-supervised physician at a medical practice is accountable for all access of HIE services by themselves and their supervised staff.

6.2.4.3 Pharmacy

A pharmacy's initial inquiries regarding connection to PharmaNet must be directed to the College of Pharmacists of BC (CPBC).

Once notified by CPBC, HIBC (Information Support) can initiate the PharmaNet connection process. All subsequent inquiries will be handled through HIBC.

6.3 Conformance Evaluation

6.3.1 Overview

To access the ministry HIE services the POS systems must comply with the HL7 messaging and transport specifications and the defined conformance standards. The POS system must pass the provincial conformance evaluation.

Conformance evaluations will:

- facilitate a fair and consistent evaluation of all software organizations' applications and processes; and
- assess whether the POS application:
  - properly implements the standards and technical specifications;
  - provides accurate and correctly interpreted data; and
  - operates efficiently with the integrated systems.

Evidence of conformance is established through attestation or submission of supporting documentation as well as demonstrable standards in a formal evaluation session.

6.3.2 Scheduling

Prior to submitting the conformance initiation document, software organizations must perform a conformance self-test against the test cases using the sandbox environment and associated data.

Software organizations must complete and submit a 'Conformance Initiation Notice' (HLTH 4636).

Four weeks of notice is required for conformance test scheduling. To assist software organizations with conformance evaluation planning, a "Conformance Information Checklist" is provided as Appendix A of this document.

6.3.3 Test Cases and Data

Test cases and related data will be provided; some data must be incorporated into the POS application prior to the scheduled test session. Test cases allow the software organization to demonstrate it meets the conformance rules, but may not reflect standard user workflow. Organizations will be required to complete and pass all provided test cases as well as message verification.

6.3.4 Self-Test

Prior to requesting a conformance evaluation, the vendor must perform a self-test using the applicable test cases for their application.

6.3.5 Evaluation

Conformance will be evaluated by one or more of the following processes:

- attestation through a signed legal agreement with the ministry; that you have conformed to the applicable standards and that documented policy and procedures are maintained for internal purposes or to support an audit;
- providing a high-level description of how your product conforms to the stated standard;
- demonstrating compliance to the stated standards;
- message level validation; and
- submission of training plans and materials.

6.3.6 Evaluation Team

The conformance evaluation team, representing the specific ministry business area, will evaluate and score the tests. Subject matter experts may also attend part of the session to provide advice and guidance in their area of expertise but will not be participating in the overall evaluation and scoring.

6.3.7 Test Scoring

A ‘pass’ or ‘fail’ will be assigned to the result of each test case based on the following scoring criteria:

- Pass: The actual result matches the expected result, which link to the conditions/rules identified in the conformance standards.
- Fail: Where any part of the test case does not meet the expected result.

If a test script is set up in a way that will not allow the software organization to execute the script in the exact sequence of steps (e.g., due to the design of their system) they may, at the discretion of the evaluators, provide an alternate set of steps to confirm the requirement.

The conformance team may, at their discretion, assign a `pass’ to the test if they have been convinced that the conformance rule(s) is met.

During the conformance test ministry representatives will document the results of each test and provide the organization a remediation report.

6.3.8 Compliance

A formal letter of compliance (known as an Interface Approval Notice) will be issued upon successful completion of all components of the conformance test including training materials evaluation, privacy and security, application enforced rules, message specifications and transport protocols.

An Interface Approval Notice will expire after five years. Organizations must notify the ministry if material changes are made to their software within the five-year period by submitting a 'Application Release Assessment' (HLTH 4635) to the Ministry's CIS Support Team. The ministry will determine the scope of conformance testing required.

To remain compliant vendor organizations will be required to implement changes to their application when advised by the ministry of updated conformance standards. A demonstration of compliance (conformance test) will be required and letter of compliance provided.

A maximum of two versions of an organizations' software will be approved to concurrently access ministry production health information exchange services for a period of six months to allow end-users to transition to the most recently approved software version.

The software organization must notify the ministry of its plan for rolling out the new software version and for transitioning its users from older software versions to the new software version. The plan must transition its users to the new software version within six months of receiving ministry approval.

6.3.9 Non-Compliant Results

When the software organization does not successfully pass the conformance test, they will be given a remediation report detailing the specific test cases and/or rules failed during the test.

Once the organization has remediated and tested the changes required a conformance evaluation can be scheduled by submitting a 'Conformance Initiation Notice' to the Ministry's CIS Support Team.

7.0 Tools for Software Organizations

7.1 HNSecure Toolkit

HNSecure is software developed by the ministry for securely exchanging electronic health information via the Internet. HNSecure performs encryption/decryption, authentication and message routing services.

HNSecure uses two software packages:

- HNClient: performs encryption, decryption, and authentication services for POS applications.
- HNServer/HNGate: does the same as well as message routing for server applications.

The HNGard infrastructure is a service that registers and validates HNSecure facilities in a directory. Information about HNSecure or the HNSecure Toolkit is available in Volume 5B.

7.2 PharmaNet API

Another way to access PharmaNet is through the PharmaNet application programming interface (API). These restful APIs are deployed using scalable container-based platform. The service is accessible through the internet subject to required authorization flows of the environment being accessed. Contact HLTH.CISSupport@gov.bc.ca for more information.

8.0 Non-Production Environment Data

This section describes non-production environments and data available to software organizations developing and testing their interface application and training their end users on its functionality.

Each provincial system (CR, PLR, PharmaNet and PLIS) has the following non-production environments that mirror the functionality of its production environment:

- **Sandbox**: Access to the sandbox environment is provided to software organizations for testing the development of an interface application. The sandbox environment will be populated with data that will support the requirements in the Volume 4 set. For any organization-specific requirements for data, refer to section 8.3.

- **Conformance**: The conformance environment is used specifically for software organizations to demonstrate their application complies with all the requirements specified in the Conformance Standards. Self-testing to validate compliance to the conformance standards will be completed in the conformance environment.

- **Training**: The training environment is used specifically to demonstrate an interface application's functionality to end users. Most significantly, it provides end users with an environment to practice tasks without being in a 'live' environment or affecting any real health information. The training environment is populated with data that supports the training requirements. For any organization-specific requirements for training data, see below.

8.1 Types of Data

8.1.1 Shared Data

Shared data is specific data created by the ministry to be used by all organizations as read-only data. It will typically be identified by specific PHNs or provider IDs. The ministry will clearly indicate which data is shared data. Because this data is shared by all organizations, any demographic and/or clinical data associated with these identifiers must NOT be modified or deleted by users or software organizations.

- **Integrated Data**: Integrated data is a specific type of shared data.
  - In the integrated dataset, a reasonable amount of data displays across all pertinent HIE services (CR, PharmaNet, PLR and PLIS) for the same patient to provide a more complex, real-world view of patient records.
- **Domain-Specific Data**: Other types of shared data are specific to a particular business domain (e.g., PharmaNet).
  - Data identified as belonging to a particular domain should be used specifically for that domain’s transactions.
  - Note that while PHNs identified for a clinical domain will also be present in the CR, they are best used for the clinical domain transactions only.

8.1.2 Organization-Specific Data

Organization-specific data is data created by the ministry to be used solely by a single organization. Organization-specific data is to be used to verify conformance standards that involve updating or deleting data. It is identified by the organization's specific usage identifier.

All organization-specific data will be identified by a 2-3 letter 'usage identifier' assigned to each software organization. This usage identifier is prepended to the last name of the demographic record.

If the software organization requires specific data created, they must direct the data request as follows:

Organization Type	Repository	Contact
Health authority	• PharmaNet • PLIS	HLTH.CISSupport@gov.bc.ca
	• Client Registry • PLR	HLTH.REGISTRIESADMIN@gov.bc.ca
Vendor (EMR)	• Client Registry • PLR	HLTH.REGISTRIESADMIN@gov.bc.ca
	• PharmaNet • PLIS	HLTH.CISSupport@gov.bc.ca
Vendor (Pharmacy)	• PharmaNet	HLTH.CISSupport@gov.bc.ca

8.1.3 Organization-Created Data

Organization-Created Data is created by the organization. It is to be used solely by the organization. When created, it must be identified as belonging to that organization by its usage identifier.

Software organizations are advised not to assign clinical data to organization-generated patient records because those records will not be recognized in the ministry systems (e.g., if a new patient is created using the Client Registry's Revise Person transaction, and the organization attempts to create a prescription for the patient, the transaction will fail with the PharmaNet error 'PHN not found').

8.2 Viewing Data

Developers will want to verify whether their application's interface functionality resulted in the desired effects to the data. Some ministry HIE services allow for an independent view of the data, while others are limited to the organization's application issuing a query.

To view data in the non-production environments, software organizations may use the following:

Repository	View Methodology
Client Registry	• The organization's application to issue query and view data. • Client Registry web application.
PLR	• PLR web application.
PharmaNet	• The organization's application to issue query and view data.
PLIS	• The organization's application to issue query and view data.

To receive access to either the Client Registry or PLR web application send an email request to HLTH.REGISTRIESADMIN@gov.bc.ca providing the:

- applicable registry (Client or Provider); and
- the user(s) information (i.e., full name, email, contact information, and role).

8.3 Triggering Data Changes

There are some specific situations in the test plans that require an action to be performed that is typically exercised independently of the application user's work flow (e.g., a prescription is issued using a medical practice application (i.e., an EMR) which then must be dispensed by someone using pharmacy software). Some of these situations can successfully be mimicked by the software organization while others require direct assistance.

Those in the latter category include:

Repository	Desired Result	Software Organization Action
Client Registry	• Merged PHN.	Send request to: HLTH.REGISTRIESADMIN@gov.bc.ca
PharmaNet	• Dispense a sample.	Issue the Medication Update – TMU transaction.
	• Reverse a sample dispense.	Issue the Medication Update Reversal – TMU transaction.
	• Dispense a prescription on a non-sample medication. • Adapt a prescription. • Reverse a dispense issued on a non-sample medication.	Send request to: PCareSupport@maximusbc.ca
PLR	• Generate a distribution.	Send request to: HLTH.REGISTRIESADMIN@gov.bc.ca
PLIS	• Update or correct a lab record. • Withdraw a report.	Send request for 'Day 2' lab data load to: HLTH.CISSupport@gov.bc.ca
	• Set a corrected or updated lab record back to its initial state. • Set a withdrawn report back to its initial state.	Send request for 'Day 1' lab data load to: HLTH.CISSupport@gov.bc.ca

8.4 Environment Data Refresh

8.4.1 Sandbox Environment

The Client Registry and PLR sandbox environments are not refreshed (base lined). Software organizations are free to manually reset their own organization-specific data to its initial state, but care must be taken if the organization's application-based data and the ministry repository data are to remain synchronized.

The PLIS environment can be refreshed to either 'Day 1' or 'Day 2' scenario data, upon request of a software organization.

8.4.2 Conformance Environment

The PharmaNet and PLIS conformance environments are refreshed (base lined) at the beginning of each conformance test; the Client Registry and PLR conformance environments are not.

8.4.3 Training Environment

The Client Registry and PLR training environments are not refreshed (base lined). Given this, the software organization must manage its organization-specific data accordingly. Software organizations are free to manually reset their own organization-specific data to its initial state, but care must be taken if the organization's application-based data and the ministry repository data are to remain synchronized.

The PLIS environment can be refreshed to either 'Day 1' or 'Day 2' scenario data, upon request by a software organization.

8.5 Quality Assurance

Ministry repositories are monitored for compliance to privacy and security standards and best practice. Where it is deemed records contained in the repositories are in contravention to any of the standards, they may be removed.

9.0 Support Model

9.1 Software Organization Non-Production Support

Prior to production, the ministry will provide Tier 1 (first line) integration support services to organizations connecting to ministry systems. These services include:

- answering queries regarding the conformance standards, conformance processes, integration requirements;
- receiving requests for connectivity, registration, access credentials and data;
- processing requests for conformance testing;
- communicating with software organizations on all incidents;
- categorizing and triaging reported incidents;
- opening tickets and providing relevant information to Tier 2 support organizations; and
- managing and closing incidents.

9.2 Software Organization Production Support

Software organizations integrating with ministry HIE services are responsible for providing Tier 1 (first line) support services for their end users for any incident related to ministry system integration including:

- communicating with users (e.g., POS clients, third party IT support) on all incidents;
- categorizing and triaging reported incidents;
- providing relevant information to third party IT support staff;
- opening tickets and communicating with Tier 2 support organizations for HIE Services; and
- managing and closing incidents with the users.

As first line of support, the organization will determine the origin of the incident and take appropriate action as described below.

Origin or Incident	Action
Client hardware, software, network infrastructure, or security software (firewall, antivirus)	• If not provided by the software organization, advise the user to contact IT support within their organization.
POS application	• Open an internal "ticket" and resolve the incident through your own support organization; • Advise users; and • Close the ticket.
HNSecure	• Open a "ticket" with the Tier 2 support organization (Ministry Help Desk): ○ 250-952-1234 or HLTH.helpdesk@gov.bc.ca; • Monitor the progress of the resolution and, if required, escalate; • Contact the originator of the call to confirm the incident was resolved to their satisfaction; and • Close the ticket with the Tier 2 support organization.

Origin or Incident	Action
Business or data incident	Contact the appropriate Tier 2 support organization on the user's behalf. PharmaNet: • 1-800-554-0225 (toll free) • 604-682-7120 (Vancouver) Client Registry and PLR: • 250-952-9137 • HLTH.REGISTRIESADMIN@gov.bc.ca PLIS: • 604-675-4299 • servicedesk@phsa.ca (Attention: VPP-eHealth Technical)
Secure Transport API Gateway	Development support for the API gateway will be managed and escalated through coordinated by CIS - HLTH.CISSupport@gov.bc.ca

9.3 Service Interruption - Production Environment

9.3.1 Regular Maintenance Windows

Production services will not be available during the regular maintenance windows:

System	Schedule	Day	Time
PharmaNet	Weekly	Thursday	12:00 am – 8:00 am
Client Registry (Legacy)	Weekly	Sunday	6:00 am – 9:00 am
PLIS	Weekly	Sunday	2:00 am – 4:00 am
	Monthly	2nd Wednesday	6:00 am – 8:00 am
Enterprise Master Patient Index (EMPI)	No scheduled outages		
PLR	No scheduled outages		

9.3.2 Unexpected/Unscheduled Maintenance Windows

Organizations will be notified of all unexpected or unscheduled outages as soon as possible through an email distribution. It is the responsibility of the software organization to ensure the ministry has its current contact information.

9.4 Service Interruption - Non-Production Environments

9.4.1 Regular Maintenance Windows

Non-production environments are supported during regular business hours, Monday - Friday and are not available during the regular non-production environment maintenance windows:

System	Schedule	Day	Time
PharmaNet (PNet) – Training	Weekly	Sun, Mon, Wed, and Fri	2:00 am to 3:00 am
		Tue and Thu	2:00 am to 9:00 am[1]
PNet – Sandbox & Conformance	N/A[2]	N/A[2]	N/A[2]
Client Registry	Weekly	Sun	12:00 am – 6:00 am
PLIS	N/A[3]	N/A[3]	N/A[3]
PLR	Weekly	Sun and Thu	12:00 am – 6:00 am

Notes:

1) PharmaNet maintenance time extended Tuesdays and Thursdays to accommodate base lining.
2) The PharmaNet sandbox and conformance non-production environments are maintained on an as required basis.
3) The PLIS non-production environments have no regularly scheduled maintenance window but will be unavailable in accordance with the PLIS release schedule. Notification of non-availability will be provided two days in advance.

9.4.2 Unexpected/Unscheduled Maintenance Windows

Software organizations will be notified of all unexpected or unscheduled outages to non-production environments (sandbox, conformance, and training) as soon as possible through an email distribution. It is the responsibility of the software organization to ensure the ministry has its current contact information.

10.0 Conformance Assurance

The assurance measures described in this section facilitate compliance to the latest published conformance standards. These processes will reduce the risk of:

- software being non-conformant as conformance standards mature; and
- data integrity or system availability issues arising in production.

10.1 Audit and Compliance Checks

Software organizations and users must sign legal agreements with the ministry prior to accessing its health information exchange systems. Among other conditions, these agreements give the ministry consent to audit the software organization and its points of service users. The terms and conditions in those agreements provide remedies the ministry can take in situations where organizations and users are found to be non-compliant with the agreements.

10.2 Restrictions of Use

POS applications developed with the functionality to integrate with ministry HIE services must not be installed at any POS location until a conformance evaluation has been conducted and a compliance letter from the ministry has been received. In addition, all required agreements must be signed.

10.3 Non-Conformance Penalties

Non-conformant software must not be released to a POS. If any such installations take place, they must be removed. If a system error or failure (i.e., ministry system time-out, table corruption) results from installed non-conformant software, the software organization may be required to pay for the resources used to rectify the situation.

Other penalties include the immediate termination of access to ministry HIE services and, where applicable, referral to the appropriate regulatory body for investigation and disciplinary action.

10.4 POS Application Version Control

A version number must uniquely identify the certified POS application. Audits will be done to ensure that the version number being used in a POS location correlates to the certified version. The POS application version number must increment when a major release is issued.

10.5 Ongoing Release Management

This section describes how release changes for certified POS applications are to be managed and implemented with respect to ministry involvement.

To ensure continued conformance, the ministry requires written notification of all POS application changes/upgrades to currently certified products. The notification details on the changes/upgrades must be reviewed and assessed by the ministry; in many cases there will be no further action required from the software organization but, in some instances, a re-conformance test will be necessary.

In all cases, the software organization must attain ministry approval prior to implementing the new release in a production environment by completing and submitting the 'Application Release Assessment' form to the Ministry's CIS Support Team.

Note: Ministry response can be expected within 7 business days.

10.5.1 POS Application Emergency Upgrades

Emergency changes made to certified POS applications must be reported to the ministry by the next business day. This is done by completing and submitting Section 4.0 of the 'Application Release Assessment' form to the Ministry's CIS Support Team.

11.0 Appendix A: Conformance Test Preparation Checklist

The following is a guide for software organizations to understand the preconditions and requirements for a conformance test:

Pre-Conformance Support Services	
□	Contact the CIS Support Team with questions regarding conformance standards, network issues, or general questions regarding readiness.
Conformance Self-Test	
□	Run a self-test (in conformance environment) using the provided test plan (if available) to confirm the application passes the rules specified in the conformance standards prior to requesting a formal ministry conformance test.
Conformance Test Request	
□	Submit a Conformance Initiation Notice to the CIS Support Team to schedule a formal conformance test.
Environment Readiness	
For applications using HNSecure:	
□	Confirm you have registered for and received the facility ID to be used for the evaluation (these are different from those used during development).
For applications using Secure Transport API Gateway:	
□	Confirm that proper access credentials, i.e., access tokens, facility ID have been provided.
Test Data	
□	Receive and add test data to the POS application prior to the evaluation.

Evaluation Location and Facilities	
□	Understand the remote facilities and tools to be used for conducting the evaluation remotely (unless an on-site evaluation is requested); and be available for a pre-test verification of the technology to be used during the conformance testing.

Software Organization Presenter Requirements	
Ensure the application presenter from the software organization is:	
□	Able to access technical support (if required).
□	Able to perform and display all required functions.
□	Able to provide screen shots upon request.
□	Available throughout the scheduled testing cycle.
□	Knowledgeable of the software product and the test cases.