



Ministry of
Health

British Columbia Professional and Software Conformance Standards for Electronic Health Information Exchange

Volume 1: Overview & Conformance Processes

Version 3.7 2026-02-20

Security Classification: Low Sensitivity

Copyright Notice

Copyright © 2026 Province of British Columbia (BC).

All rights reserved.

This material is owned by the Government of BC and protected by copyright law.

It may not be reproduced or redistributed without the prior written permission of the Province of BC.

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 BC 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 BC has been specifically advised of the possibility of such damages.

Document Details

Author: Ministry of Health (HLTH)

Last Updated: 2026-02-20

Version: 3.7

Table of Contents

1.0	Introduction	5
1.1	Key to Document Terminology	5
1.2	Conformance, Integration & Standards (CIS) Team	5
1.3	Audience	5
2.0	Ministry Health Information Exchange (HIE) Services	6
2.1	PharmaNet.....	6
2.2	Provider and Location Registry (PLR).....	6
2.3	Provincial Client Registry (PCR).....	7
2.4	Provincial Laboratory Information Solution (PLIS)	7
3.0	Ministry HIE Transport Protocols	8
4.0	Forms & Agreements	9
4.1	For Vendors.....	9
4.2	For Connected Parties (Users and Organizations).....	9
5.0	Conformance Standards Overview.....	10
5.1	Common Volumes	10
5.2	Domain-Specific Volumes	11
5.3	Transport Protocol Volumes.....	12
5.4	Changes to the Conformance Standards	12
6.0	Integration Processes	13
6.1	Apply for Integration Services	14
6.2	Register for Ministry System Access.....	14
6.2.1	Ministry Service Access Prerequisites	15
6.2.2	Environment Access Prerequisites	16
6.2.3	Software Organization Registration	17
6.2.4	POS User Registration.....	17
6.3	Conformance Evaluation	19
6.3.1	Overview	19
6.3.2	Scheduling.....	19
6.3.3	Test Cases and Data	19
6.3.4	Self-Test	20
6.3.5	Evaluation	20
6.3.6	Evaluation Team	20
6.3.7	Test Scoring.....	20
6.3.8	Compliance	21
6.3.9	Non-Compliant Results	21
7.0	Non-Production Environment Data.....	22
7.1	Types of Data	22

7.1.1	Shared Data	22
7.1.2	Organization-Specific Data	23
7.1.3	Organization-Created Data	23
7.2	Viewing Data	24
7.3	Triggering Data Changes	25
7.4	Environment Data Refresh	25
7.4.1	Sandbox Environment	25
7.4.2	Conformance Environment	26
7.4.3	Training Environment	26
7.5	Quality Assurance	26
8.0	Support Model	27
8.1	Software Organization Non-Production Support	27
8.2	Software Organization Production Support	28
8.3	Service Interruption – Production Environment	29
8.3.1	Regular Maintenance Windows	29
8.3.2	Unexpected/Unscheduled Maintenance Windows	29
8.4	Service Interruption – Non-Production Environments	30
8.4.1	Regular Maintenance Windows	30
8.4.2	Unscheduled Maintenance Windows	30
9.0	Conformance Assurance	31
9.1	Audit and Compliance Checks	31
9.2	Restrictions of Use	31
9.3	Deployment of Conformant Software	32
9.4	Non-Conformance Penalties	32
9.5	POS Application Version Control	32
9.6	Ongoing Release Management	33
9.6.1	POS Application Emergency Upgrades	33
10.0	Appendix A: Conformance Test Preparation Checklist	34

1.0 Introduction

Organizations developing interfaces to health information exchange (HIE) services offered by the Ministry of Health (the “ministry”) must comply with the BC Professional and Software Conformance Standards.

The Conformance, Integration & Standards (CIS) team coordinates registration, connectivity, conformance testing, and certification for applications integrating with ministry HIE services.

This document explains the purpose of the conformance standards and how they apply to organizations integrating with ministry HIE services.

1.1 Key to Document Terminology

This document and the associated conformance standards use the following terminology conventions:

- **Must, will, minimum, mandatory** – indicate a required function or requirement which must be confirmed and correctly implemented.
- **Optional** – indicates a recommended function or requirement. If implemented, it will be tested for compliance.
- Acronyms and abbreviations are defined at first use and listed in the Glossary of Terms (published separately).

1.2 Conformance, Integration & Standards (CIS) Team

For questions about conformance processes, standards, setup, or testing contact the CIS team at:

- HLTH.CISSupport@gov.bc.ca

1.3 Audience

This volume is intended for:

- Software vendors and health organizations developing interfaces to ministry HIE services.
- Health care providers and organizations that access or exchange health information from ministry or provincial data repositories
- Ministry information owners, conformance evaluation teams, and audit teams.

2.0 Ministry Health Information Exchange (HIE) Services

This section describes the ministry's HIE services available for integration with point of service (POS) applications.

2.1 PharmaNet

PharmaNet is BC's provincial drug information and claims processing system. It records all prescription dispensed by community pharmacies in BC. It is also used by health professionals in other settings for electronic prescribing and assessment of medication use.

Authorized users (e.g., pharmacists and other health professionals) can:

- Submit prescription, dispense, and claim information;
- Access and update patient medication histories (including 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.

2.2 Provider and Location Registry (PLR)

The PLR is the authoritative registry of BC health care providers' demographic and professional information (e.g., name, identifiers, demographics, expertise, contact information, licensing status, work location). It supports provider directories and activities such as referrals and consultations.

Authorized users can:

- Search the PLR for provider demographic and professional information;
- Store results in their local application for reference;
- Receive real-time distributions to maintain accurate provider directories; and
- Update provider work location details in the PLR.

2.3 Provincial Client Registry (PCR)

The PCR is the authoritative registry of health care client demographic information in BC including:

- **Identifiers** – Personal Health Number (PHN), and health authority source system identifiers (e.g., medical record number);
- **Demographics** – Name, gender, date of birth, and date of death (if applicable); and
- **Contact Information** – Address, and phone 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 can:

- Search and capture patient identity information to support safe health care service delivery;
- Store patient demographics from the PCR in their POS application;
- Update patient demographic details in the PCR; and
- Create PHNs for new patients.

Note(s): Every BC health care recipient must have a PHN.

2.4 Provincial Laboratory Information Solution (PLIS)

The PLIS contains comprehensive diagnostic laboratory test results from private and public labs across BC. It enables authorized care providers to access their patients' historical and recently published lab test results, reducing duplicate testing, and supporting timely clinical decisions.

Authorized users can:

- View a summary of all lab results for a specified period for a patient;
- Retrieve selected lab results reports; and
- Store lab results data in the local software for other clinical decision support purposes (e.g., trending, graphing).

Note(s): Integration with PLIS is currently on hold until further notice.

3.0 Ministry HIE Transport Protocols

The ministry provides secure, message-based access to HIE services for pharmacies, medical practices, and health authority facilities. All messages are standardized, secure and authenticated.

Connection methods include:

- Health Registries Broker (for PLR and PCR integrations)
- PharmaNet Application Program Interface (API) Gateway

4.0 Forms & Agreements

Organizations must complete specific forms and agreements before integrating with ministry HIE services. Requirements vary by organization type and the services accessed.

4.1 For Vendors

- Submit all required forms and agreements available at:

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

4.2 For Connected Parties (Users and Organizations)

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

- PharmaNet: Site Registration and User Agreements
- PLR, PCR, and PLIS: Information Sharing Agreements (for Health Authorities)

5.0 Conformance Standards Overview

The conformance standards are the primary reference for organizations integrating POS applications with ministry HIE services.

Organizations must:

- Access the latest conformance standards at:

<https://www2.gov.bc.ca/gov/content/health/practitioner-professional-resources/software/conformance-standards>
- Comply with applicable legislation and the published conformance standards.
- Review all volumes as a complete set (i.e., common, domain-specific, and transport protocol standards) including business rules, application enforced rules, and technical message specifications.

Integration ensures safe, efficient exchange of demographic and clinical information across BC's health care system.

5.1 Common Volumes

The following common volumes apply to all organizations:

Document	Purpose
Volume 1: Overview & Conformance Processes	<ul style="list-style-type: none"> • Explains integration processes, conformance evaluation, roles, registration, legal agreements, connectivity, and system management.
Volume 2: Information Privacy & Security	<ul style="list-style-type: none"> • Outlines the information privacy and security controls required for HIE access.
Volume 3A: Business Rules – General	<ul style="list-style-type: none"> • Defines general business and training rules for POS users.
Volume 4A: Application Enforced Rules – General	<ul style="list-style-type: none"> • Specifies application rules POS systems must enforce for all domains.
Glossary of Terms	<ul style="list-style-type: none"> • Provides definitions for terms and acronyms used in the standards.

5.2 Domain-Specific Volumes

Domain-specific volumes include:

Volume 3: Business Rules

- Defines the business and training rules for each ministry domain:
 - Volume 3B: Business Rules – PCR
 - Volume 3C: Business Rules – PharmaNet
 - Volume 3D: Business Rules – PLR
 - 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 for each ministry domain:
 - Volume 4B: Application Enforced Rules – PCR
 - Volume 4C: Application Enforced Rules – PharmaNet
 - Volume 4D: Application Enforced Rules – PLR
 - Volume 4E: Application Enforced Rules – PLIS

The following identifies the required 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
PharmaNet	✓	✓	✓		✓			✓		✓		
PLR	✓	✓	✓			✓		✓			✓	
PCR	✓	✓	✓	✓				✓	✓			
PLIS	✓	✓	✓				✓	✓				✓

Note(s): In addition, refer to the documentation for the appropriate transport protocol (e.g., Volume 5C: API Gateway).

5.3 Transport Protocol Volumes

Volume 5: Transport Protocols

Transport protocol volumes describe the technical methods for connecting POS systems to HIE services. Each protocol has its own standards and message specifications (e.g., Volume 5C: API Gateway).

5.4 Changes to the Conformance Standards

The conformance standards are:

- Updated as needed to reflect changes in legislation, policy, best practices, and HIE services;
- Published as a set of related volumes with a common version and release date; and
- Available on the ministry website.

Sign-up to receive update notifications by emailing the CIS team at: HLTH.CISSupport@gov.bc.ca.

6.0 Integration Processes

This section describes the processes for integrating POS applications with ministry HIE services, including registration, environment access, and conformance evaluation.

The following table summarizes the key participants and their responsibilities in the integration and conformance processes.

Note(s): For additional details, refer to the subsequent sub-sections.

Table 2 Roles and Responsibilities

Roles	Key Responsibilities
Ministry CIS Team	<ul style="list-style-type: none"> • Coordinate and oversee the conformance evaluation; • Coordinate/facilitate connectivity (e.g., network, ministry environments); • Issue conformance certification; • Maintain a registry of certified applications; • Provide test case support; • Maintain and publish and conformance standards and education material; and • Receive and facilitate responses to software organizations' questions and issues.
Ministry Domain Evaluation Team(s)	<ul style="list-style-type: none"> • Prepare and validate test cases (including test data); • Confirm compliance; • Approve conformance test results.

Roles	Key Responsibilities
Software Organizations (e.g., health authorities, vendors)	<ul style="list-style-type: none"> • Participate in a vendor discovery session to review integration objectives and timelines with the ministry; • Review all applicable ministry standards and requirements; • Complete self-assessment to validate developed functionality prior to requesting formal conformance testing with the ministry; • Establish secure connections to ministry network and environments); • Manage security configurations (e.g., user IDs, server certificates for environments); • Confirm all pre-requisites are met prior to conformance testing (e.g., load test data into POS application); • Demonstrate compliance with the conformance standards; • Provide client support (e.g., user registration, technical support, application training); • Submit all required forms and agreements.

6.1 Apply for Integration Services

Software organizations must complete the following steps to apply for integration with ministry HIE systems:

- Review integration requirements (e.g., options, conformance standards, and legal agreements);
- Complete and submit the Request for Integration Services form to the CIS team; and
- Participate in a vendor discovery session to:
 - Ensure integration plans align with ministry objectives;
 - Confirm understanding of the requirements;
 - Identify any constraints; and
 - Determine the appropriate integration approach and readiness.

6.2 Register for Ministry System Access

Software organizations must register for access to ministry HIE environments before conformance testing and integration. This section outlines prerequisites and registration steps for service access, environment access, and user registration.

6.2.1 Ministry Service Access Prerequisites

6.2.1.1 For Software Organizations

Software organizations must:

- Adhere to privacy and security obligations (Vol. 2);
- develop software that implements application enforced rules (Vol. 4);
- Ensure users comply with business rules (Vol. 3);
- Follow processes outlined in this document;
- Implement technical mechanisms for connectivity (Vol. 5);
- Complete the conformance process; and
- adhere to legislation and signed agreements (e.g., Vendor Participation Agreement).

6.2.1.2 For POS Application Users

POS application users must:

- Access ministry HIE services using ministry-certified software;
- Follow registration processes and business rules (Vol. 3);
- Complete training; and
- Sign required agreements.

6.2.2 Environment Access Prerequisites

6.2.2.1 Sandbox

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

Software organizations must complete the following for access:

- Review all applicable conformance standards and message specifications;
- Subscribe to vendor notifications regarding changes to the conformance standards;
- Commit to all requirements for integration with ministry HIE systems;
- Submit the [Request for Integration Services \(HLTH 4637\)](#) form;
- Agree to appropriate sandbox environment usage;
- Sign a vendor participation agreement;
- Configure the POS system for connectivity.

6.2.2.2 Conformance

The conformance environments are used by software organizations to demonstrate compliance to the conformance standards.

Software organizations must complete the following for access:

- Agree to appropriate conformance environment usage;
- Submit a [Conformance Initiation Notice \(HLTH 4636\)](#);
- Configure the POS system for connectivity; and
- Conduct a self-test to validate compliance.

Note(s): 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

The training environment is used to conduct ongoing end user training.

Software organizations must complete the following for access:

- Configure the POS system for connectivity;
- Confirm vendor registration and provide a privacy contact;
- Receive ministry certification; and
- Understand and use the ministry support model.

6.2.3 Software Organization Registration

The CIS team coordinates access to the ministry's sandbox, conformance, training, and production environments. Software organizations must:

- Register for integration services using the appropriate forms (based on system type and desired HIE access);
- Provide required configuration details for secure network access; and
- Contact the CIS team for guidance at: HLTH.CISSupport@gov.bc.ca.

6.2.4 POS User Registration

The user registration process to access HIE systems in a production environment depends upon the POS and the HIE system.

6.2.4.1 Health Authority Users

- For PLR, PCR, and PLIS – Each health authority must manage their users and access to ministry systems (e.g., approvals, reviews, breach management, and training).
- For PharmaNet – Health authority users must enroll in PRIME and receive ministry approval.

6.2.4.2 Medical Practice Users

- For PharmaNet – Medical practices must register all sites, enrol all users in PRIME, and receive ministry approval.
 - User access requires technical configuration changes to be implemented by both the POS software provider and the ministry.
 - Software organizations may want to prompt the medical practice to register to expedite the process.
 - The authorized practitioner providing care to the individual whose records are being accessed is responsible for their own use of PharmaNet and for that of any individuals acting on their behalf.
- For PLR, PCR and PLIS – Each non-supervised physician at a medical practice is accountable for all access by themselves and their supervised staff.

6.2.4.3 Pharmacy Users

- For PharmaNet – A pharmacy’s initial inquiries regarding connection and registration of a site to PharmaNet must be directed to the ministry.
 - Pharmacy users must enrol in PRIME and receive ministry approval.

6.3 Conformance Evaluation

6.3.1 Overview

POS systems must comply with applicable business rules, application enforced rules, privacy and security, and transport/message specifications. Conformance is established through documentation/attestation, message-level validation, and demonstration during formal conformance evaluation.

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 a Conformance Initiation Notice (CIN) to schedule formal conformance testing, organizations must complete conformance self-testing using the appropriate test cases, data, and environment.

Once ready to proceed, the CIN must be submitted to the CIS team.

A minimum of four weeks notice is required to schedule formal conformance testing, and typical evaluation duration is 3-8 business days. A "Conformance Information Checklist" is provided as Appendix A of this document to assist software organizations with conformance evaluation planning.

6.3.3 Test Cases and Data

The ministry provides test cases and related data. Some data must be pre-loaded into the POS application prior to testing. Test cases validate conformance rules and may not match standard user workflows.

6.3.4 Self-Test

Mandatory – The vendor must fully complete self-testing and resolve issues before requesting formal conformance evaluation.

6.3.5 Evaluation

Evaluation may include:

- attesting compliance through a signed legal agreement confirming adherence to the applicable standards and maintenance of required policies and procedures;
- providing a high-level description of how the product meets each stated standard;
- demonstrating compliance by executing required workflows and functions during the conformance evaluation;
- validating messages against specifications and conformance rules; and
- submitting training plans and materials for review to ensure user readiness and compliance with business rules.

Organizations must also complete privacy/security gap analysis, and if applicable, the cloud security schedule (HLTH 801).

6.3.6 Evaluation Team

The Ministry team (including subject matter experts as required) will complete the conformance evaluation.

6.3.7 Test Scoring

Each test case is scored Pass/Fail:

- 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 incompatible with the POS design, evaluators may accept alternate steps if the requirement is fully demonstrated.

Results and any required steps for remediation will be documented in the conformance evaluation report.

6.3.8 Compliance

If all requirements are met, the ministry will issue an Interface Approval Notice or “IAN” (which is valid for 5 years).

Organizations must:

- Notify the ministry if material changes are made to their software within the five-year approval period by submitting an Application Release Assessment or “ARA” (HLTH 4635) to the CIS team.
- Allow the ministry to determine the scope of conformance testing required for those changes.
- Implement changes to their application when advised of updated ministry conformance standards.
- Demonstrate compliance through conformance testing and obtain a new IAN.
- Ensure no more than two versions of their software are concurrently accessing ministry production HIE services, and limit any overlap to six months to allow end-users to transition to the most recently approved software version.
- Notify the ministry of their rollout plan for deploying the new software version and transitioning users from older versions.
- Complete the transition of all users to the new software version within six months of receiving ministry approval.

6.3.9 Non-Compliant Results

If an organization does not successfully pass the conformance test, the ministry will issue a remediation report detailing all failed test cases and the corresponding conformance rules.

The organization must correct the identified issues, perform internal testing, and complete a self-test in the appropriate ministry environment to confirm readiness. Once these steps are completed, the organization can request a re-evaluation by submitting a new “CIN” to the CIS team, ensuring the required notice period is met.

7.0 Non-Production Environment Data

This section describes the non-production environments available for software organizations to develop, test, and train on their interface applications.

Each provincial HIE system (i.e., PharmaNet, PLR, PCR and PLIS) provides non-production environments that mirror production functionality:

Environment	Notes
Sandbox	<ul style="list-style-type: none"> Used for development and internal testing. Pre-populated with data supporting conformance requirements.
Conformance	<ul style="list-style-type: none"> Used to demonstrate compliance with the ministry’s conformance standards. This includes mandatory self-testing.
Training	<ul style="list-style-type: none"> Used for end-user training and practice without impacting the “live” production environment or actual health information. Populated with data supporting training scenarios.

7.1 Types of Data

The ministry provides three categories of data in non-production environments.

7.1.1 Shared Data

Shared data is created by the ministry for use by all organizations as **read-only**. These records are identified by specific PHNs or provider IDs and must not be modified or deleted.

- Integrated Data:** A subset of shared data that spans multiple HIE services for the same patient, providing a realistic view of cross-domain records.
- Domain-Specific Data:** Shared data for a single domain (e.g., PharmaNet) and intended for domain-specific transactions.

7.1.2 Organization-Specific Data

Organization-specific data is created by the ministry for use by a single organization to verify conformance standards that involve updating or deleting data.

This data is identified by the organization's specific usage identifier (i.e., 2-3 letters assigned to each software organization) which is then prepended to the surname of the demographic record.

Requests for organization-specific data must be directed as follows:

Contacts:

- PharmaNet / PLIS = HLTH.CISSupport@gov.bc.ca
- PLR / PCR = HLTH.REGISTRIESADMIN@gov.bc.ca

7.1.3 Organization-Created Data

Organization-created data is introduced by the vendor or connected party for exclusive use by that organization. These records must:

- be tagged with a unique identifier (e.g., Surname = FHADictionary, Surname = PHSASWord); and
- not be assigned clinical data since they will not be recognized across ministry systems (e.g., if a new patient is created using the PCR'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').

7.2 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.

Organizations can verify data changes using the following:

Repository	Method
PharmaNet	<ul style="list-style-type: none"> Issue queries through the POS application.
PCR	<ul style="list-style-type: none"> Issue queries through the POS application or use the PCR web application.
PLR	<ul style="list-style-type: none"> Use the PLR web application.
PLIS	<ul style="list-style-type: none"> Issue queries through the POS application.

Access requests for the PLR or PCR web application must be submitted to HLTH.REGISTRIESADMIN@gov.bc.ca providing the:

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

7.3 Triggering Data Changes

Some test scenarios require actions outside normal workflows (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. If the software organization is unable to mimic the situation, they must reach out to following contacts:

Repository	Desired Result	Software Organization Action
PharmaNet	<ul style="list-style-type: none"> Dispense or reverse a sample. 	Issue TMU or TMU reversal transaction.
	<ul style="list-style-type: none"> Dispense/adapt/reverse a non-sample medication. 	Send request to: pcareqa@hibc.gov.bc.ca
PLR	<ul style="list-style-type: none"> Generate a distribution. 	Send request to: HLTH.REGISTRIESADMIN@gov.bc.ca
PCR	<ul style="list-style-type: none"> Merge PHN. 	Send request to: HLTH.REGISTRIESADMIN@gov.bc.ca
PLIS	<ul style="list-style-type: none"> Update/correct lab record or withdraw report. 	Send request (for Day 2 data load) to: HLTH.CISSupport@gov.bc.ca
	<ul style="list-style-type: none"> Reset corrected/withdrawn record to initial state. 	Send request (for Day 1 data load) to: HLTH.CISSupport@gov.bc.ca

7.4 Environment Data Refresh

Non-production environments follow different refresh policies. Organizations must plan accordingly to maintain data integrity and synchronization between their POS application and ministry repositories.

7.4.1 Sandbox Environment

The PLR and PCR sandbox environments are not re-baselined (i.e., refreshed). Software organizations may manually reset their own organization-specific data to its initial state, but must ensure synchronization between their application-based data and ministry repository data.

The PLIS sandbox environment can be re-baselined to either 'Day 1' or 'Day 2' scenario data upon request.

7.4.2 Conformance Environment

The PharmaNet and PLIS conformance environments are re-baselined at the start of each conformance test to ensure consistency for evaluation.

The PLR and PCR conformance environments are not re-baselined.

7.4.3 Training Environment

The PLR and PCR training environments are not re-base lined. Organizations must manage organization-specific data and ensure synchronization between their application and ministry repositories.

The PLIS training environment can be refreshed to either 'Day 1' or 'Day 2' scenario data upon request.

7.5 Quality Assurance

Ministry repositories are monitored for compliance with privacy and security standards and best practice. Records found to contravene these standards or best practices may be removed.

8.0 Support Model

The ministry and software organizations share responsibilities for support across non-production and production environments.

8.1 Software Organization Non-Production Support

Prior to production, the ministry will provide Tier 1 integration support to organizations connecting to ministry systems.

These services include:

- Responding to queries about conformance standards, processes, and integration requirements;
- Processing requests for connectivity, registration, access credentials, and test data;
- Scheduling and coordinating conformance testing;
- Logging and triaging reported incidents;
- Escalating issues to Tier 2 support organizations as needed; and
- Managing and closing incidents.

8.2 Software Organization Production Support

Software organizations must provide Tier 1 support for end users in production environments.

Responsibilities include:

- 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 internal tickets and resolving POS application issues;
- Communicating with Tier 2 support organization; and
- Managing and closing incidents with users.

As the first line of support, the organization must identify the source of the incident and take the appropriate corrective action or escalation steps as outlined below.

Origin or Incident	Action
Client hardware, software, network infrastructure, or security software (firewall, antivirus)	<ul style="list-style-type: none"> • Advise the user to contact their internal IT support if these services are not provided by the software organization.
POS application	<ul style="list-style-type: none"> • Open an internal support ticket, resolve the issue through your support team, inform the user of the resolution, and close the ticket.
Business or data incident	<p>Collect all relevant details, escalate the issue to the appropriate Tier 2 support organization, and communicate updates to the user.</p> <ul style="list-style-type: none"> • For PharmaNet: Call 1-800-554-0225 (toll free) or 604-682-7120 (Vancouver). • For PLR and PCR: Call 250-952-9137 or email HLTH.REGISTRIESADMIN@gov.bc.ca. • For PLIS: Call 604-675-4299 or email servicedesk@phsa.ca (Attention: VPP-eHealth Technical).

8.3 Service Interruption – Production Environment

8.3.1 Regular Maintenance Windows

Production services will not be available during the regular maintenance windows. All times are Pacific Time (PT).

System	Schedule	Day	Time (PT)
PharmaNet	Weekly	Thursday	00:00 – 08:00
PLR	No scheduled outages	N/A	N/A
PCR	Weekly	Sunday	06:00 – 09:00
PLIS	Weekly	Sunday	02:00 – 04:00
PLIS	Monthly	2nd Wednesday	06:00 – 08:00

8.3.2 Unexpected/Unscheduled Maintenance Windows

Organizations will be notified of outages via email and must ensure the CIS team has current contact information.

8.4 Service Interruption – Non-Production Environments

8.4.1 Regular Maintenance Windows

Non-production environments are supported during regular business hours, Monday to Friday and are not available during the regular non-production environment maintenance windows. All times are Pacific Time (PT).

System	Schedule	Day	Time (PT)
PharmaNet			
• Sandbox (VS1) & Conformance (VC1/VC2)	Ad hoc	—	—
• Training (TRN1)	Weekly	Tue	03:00 – 08:30
PLR	Weekly	Sun & Thu	00:00 – 06:00
PCR	Weekly	Sun	00:00 – 06:00
PLIS	Ad hoc	—	—

Note(s): The PLIS non-production environments have no regular maintenance window but may be unavailable per release schedule with notice provided at least two days in advance.

8.4.2 Unscheduled Maintenance Windows

Organizations will be notified of outages via email. It is the responsibility of the software organization to ensure the ministry has its current contact information.

9.0 Conformance Assurance

The assurance measures in this section ensure ongoing compliance with the latest published conformance standards. These processes reduce the risk of:

- Software becoming non-conformant as standards evolve; and
- Data integrity issues or system availability issues arising in production.

9.1 Audit and Compliance Checks

Software organizations and users must sign all required legal agreements before accessing ministry HIE systems. These agreements give the ministry consent to audit the software organization and POS users. They also outline remedies for non-compliance, which may include suspension of access or other corrective actions.

Organizations should support audit readiness by:

- Maintaining training records and user access logs;
- Retaining documentation of conformance test results and release approvals; and
- Ensuring version control and deployment records are up to date.

9.2 Restrictions of Use

All required agreements must be signed and 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.

9.3 Deployment of Conformant Software

Organizations must deploy conformant software to all sites within six months of receiving ministry approval. The ministry may require a shorter deployment period in specific cases.

Software organizations must:

- Inform all their client organizations of this requirement; and
- Initiate change management with the appropriate ministry business area:
 - PharmaNet – Health System Policy & Oversight (HSPO)
 - PLR – Health Registries
 - PCR – Health Registries
 - PLIS – HSPO

If conformance standards change, deployment timelines may be adjusted in consultation with the ministry and the relevant business areas. For larger updates to conformance the associated ministry business area may work with vendors and client organizations on a deployment schedule.

9.4 Non-Conformance Penalties

Non-conformant software must never be deployed to production. If discovered, it must be removed immediately. Penalties for non-compliance may include:

- Cost recovery for resources used to resolve resulting system issues (e.g., ministry system time-out, table corruption);
- Immediate termination of access to ministry HIE services; and/or
- Referral to regulatory bodies for investigation and disciplinary action.

Unauthorized HIE system access may also result in removal of access and further investigation.

9.5 POS Application Version Control

Certified POS applications must be uniquely identified by a version number. Audits will verify that the version deployed matches the certified version. The version number must be incremented for every major release.

9.6 Ongoing Release Management

Organizations must:

- Notify the ministry of all changes to certified POS applications by submitting an Application Release Assessment ([ARA](#)); and
- Attain ministry approval before deploying any new release in production.

The ministry will review the changes and respond within seven business days, indicating whether re-conformance testing is required.

It is suggested that organizations prepare for software releases by:

- Documenting the:
 - change description and scope including the impacted domains, and
 - privacy/security implications;
- Updating training materials; and
- Preparing a proposed deployment schedule.

9.6.1 POS Application Emergency Upgrades

Emergency changes must be reported to the ministry by the next business day using Section 4.0 of the '[Application Release Assessment](#)' (HLTH 4635). Emergency releases must still comply with all privacy and security requirements outlined in Volume 2.

10.0 Appendix A: Conformance Test Preparation Checklist

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

Conformance Test Preparation Checklist	
Pre-Conformance Support Services	
<input type="checkbox"/>	Contact the CIS team with questions about conformance standards, network issues, or readiness.
Conformance Self-Test	
<input type="checkbox"/>	Run a self-test in the assigned conformance environment using the provided test plan (if available) to confirm the application meets conformance standards before a formal conformance test.
Conformance Test Request	
<input type="checkbox"/>	Submit a Conformance Initiation Notice to the CIS team to schedule a formal conformance test.
Environment Readiness - For applications using Secure Transport API Gateway:	
<input type="checkbox"/>	Confirm that access credentials (e.g., tokens, facility ID) have been provided.
Test Data	
<input type="checkbox"/>	Add test data to the POS application before the evaluation.
Evaluation Setup and Readiness	
<input type="checkbox"/>	Confirm remote facilities and tools (unless an on-site evaluation is requested) and participate in a pre-test technology check with the Ministry team.
Software Organization Presenter Requirements	
Confirm the presenter representing the software organization is able to:	
<input type="checkbox"/>	Access technical support (if required).
<input type="checkbox"/>	Perform and display all required functions.
<input type="checkbox"/>	Provide screenshots upon request.
<input type="checkbox"/>	Demonstrate knowledgeable of the software product and test cases.