



Ministry of  
Health

British Columbia  
Professional and Software Conformance Standards

Electronic Health Information Exchange  
Volume 1: Overview and Conformance Processes

Version 2.0 2017-03-31

Security Classification: Low Sensitivity

---

#### 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.

Author:	MoH Conformance Services
Date Created:	2011-03-04
Last Updated:	2017-03-31
Version:	2.0

---

## Table of Contents

<b>1.0</b>	<b>Introduction</b>	<b>5</b>
1.1	Key to Document Terminology	5
1.2	Ministry of Health Conformance Standards Contact	5
1.3	Audience	5
<b>2.0</b>	<b>Ministry Health Information Exchange Services</b>	<b>6</b>
<b>3.0</b>	<b>Conformance Standards Overview</b>	<b>9</b>
3.1	Common Volumes	9
3.2	Domain Specific Volumes	10
3.3	Transport Protocol Volumes	10
3.4	Required Conformance Standards by Service Integration	11
3.5	Changes to the Conformance Standards	11
<b>4.0</b>	<b>Integration Processes</b>	<b>12</b>
4.1	Apply for Integration Services	13
4.2	Register for Ministry System Access	14
4.2.1	Ministry Service Access Prerequisites	14
4.2.2	Environment Access Prerequisites	15
4.2.3	Software Organization	16
4.2.4	POS User Registration	17
4.3	Evaluation and Compliance	18
4.3.1	Overview	18
4.3.2	Scheduling	18
4.3.3	Test Cases and Data	19
4.3.4	Evaluation	19
4.3.5	Evaluation Team	19
4.3.6	Test Scoring	19
4.3.7	Evaluation Results	20
4.3.8	Compliance	20
4.3.9	Non-Compliant Results	20
<b>5.0</b>	<b>Agreements</b>	<b>21</b>
5.1	Circuit Orders and Connection Agreements (for HIAL access only)	21
5.2	Vendor Participation Agreement	21
5.3	Information Sharing Agreements - Health Authorities	21
<b>6.0</b>	<b>Tools for Software Organizations</b>	<b>22</b>
6.1	EMR Reference Implementation	22
6.2	HNSecure Toolkit	22
<b>7.0</b>	<b>Non-Production Environment Data</b>	<b>23</b>

---

---

7.1	Overview.....	23
7.2	Types of Data.....	23
7.2.1	Shared Data .....	23
7.2.2	Organization-Specific Data .....	24
7.2.3	Organization-Created Data.....	24
7.3	Viewing Data.....	25
7.4	Triggering Data Changes.....	25
7.5	Environment Data Refresh .....	26
7.5.1	Sandbox Environment .....	26
7.5.2	Conformance Environment .....	27
7.5.3	Training Environment .....	27
7.6	Quality Assurance.....	27
<b>8.0</b>	<b>Support Model.....</b>	<b>28</b>
8.1	Software Organization Non-production Support .....	28
8.2	Software Organization Production Support .....	28
8.3	Service Interruption - Production Environment .....	30
8.3.1	Regular Maintenance Windows .....	30
8.3.2	Unexpected/Unscheduled Maintenance Windows.....	31
8.4	Non-Production Environments.....	31
8.4.1	Regular Maintenance Windows .....	31
8.4.2	Unexpected/Unscheduled Maintenance Windows.....	31
<b>9.0</b>	<b>Continued Conformance .....</b>	<b>32</b>
9.1	Audit and Compliance Checks .....	32
9.2	Restrictions of Use.....	32
9.3	Non-Conformance Penalties.....	32
9.4	POS Application Version Control .....	32
9.5	Ongoing Release Management .....	32
9.5.1	POS Application Emergency Upgrades .....	33
<b>Appendix A: Conformance Test Preparation Checklist .....</b>		<b>34</b>
<b>Appendix B: Forms .....</b>		<b>35</b>

---

## 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 team 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:

- 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.
- 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.
- 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.

A Glossary of Terms is provided in a separate volume of the conformance standards. 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.

### 1.2 Ministry of Health Conformance Standards Contact

Questions regarding the conformance standards should be directed to the ministry at:  
[HLTH.CISSupport@gov.bc.ca](mailto: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 Services

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 *Health Information Access Layer (HIAL)* or HNSecure to exchange healthcare information between a *Point of Service (POS)* and ministry domain system. The HIAL is a communication and message management service supporting the secure and auditable exchange of healthcare information between a POS and ministry systems. 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 Application Program Interface (API) to access the PharmaNet system.

Within the scope of the conformance standards is the access/exchange of *electronic health information* between POS and ministry systems:

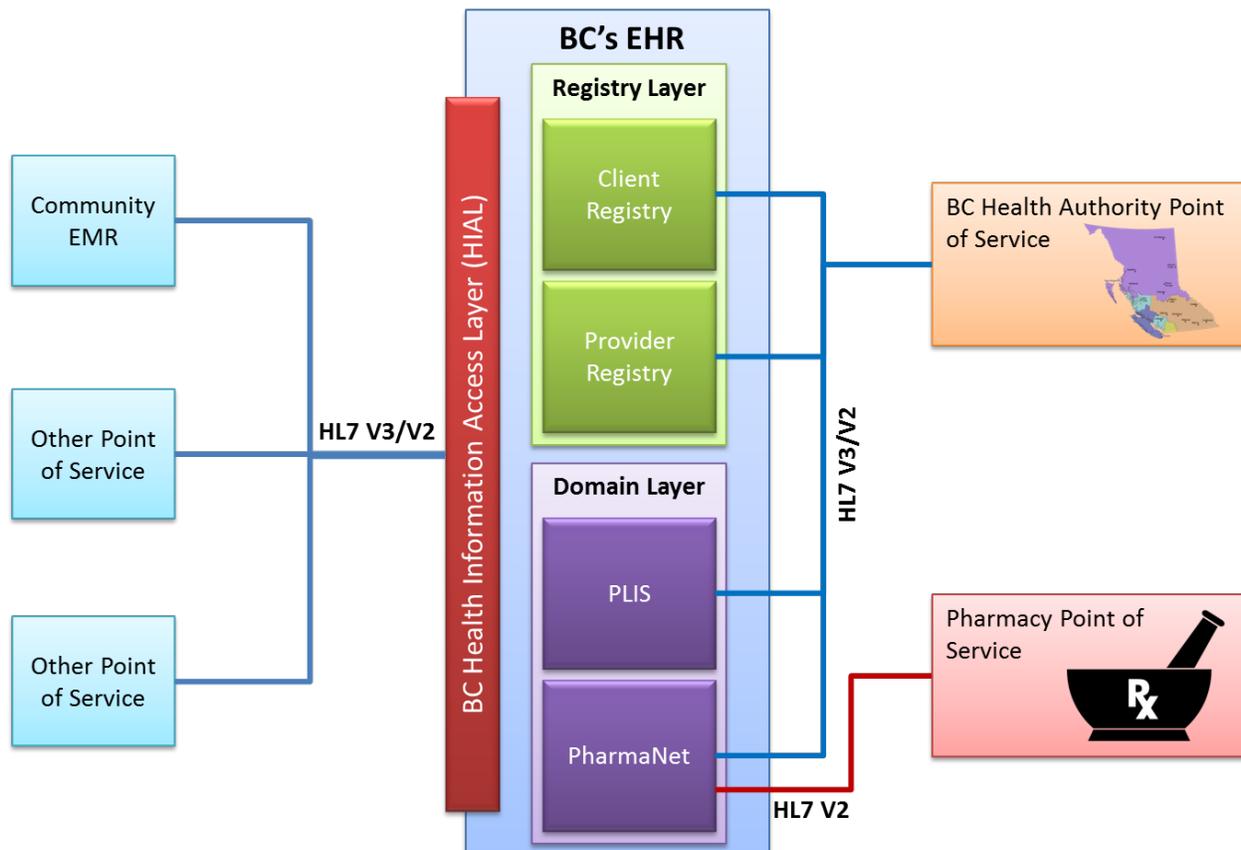


Figure 1 Ministry Health Information Exchange Overview

Electronic health information in the following ministry systems is made available to POS systems:

The **Client Registry (CR)** is the authoritative registry of healthcare client *demographic information* in British Columbia. This includes the 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 care and safe health service delivery;
- store client demographics from the CR in the POS application;
- update client demographic information in the Client Registry; and
- create a PHN for patients, ensuring every recipient of BC healthcare services has one.

The **Provider Registry (PR)** is the authoritative registry of British Columbia health care providers' demographic and professional information (e.g., name, identifiers, demographics, expertise, contact and licensing status). This information can be used to maintain internal provider directories within the health sector. The registry also supports activities such as patient referrals and informal consultations between care providers.

Authorized users with a POS application integrated with the PR 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 Provider Registry.

**PharmaNet** is the provincial drug information and claims processing system that links all community pharmacies in British Columbia. It contains every prescription dispensed by community pharmacies in B.C. PharmaNet helps pharmacists and other health professionals identify and warn patients about potentially harmful medication interactions, unintended duplications, and risks from the misuse of prescription drugs.

Authorized users 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; and

- monitor patient medication adherence by verifying the status of a prescription.

The **Provincial Laboratory Information Solution** (PLIS) contains comprehensive diagnostic laboratory test results from private and public laboratories across British Columbia. It 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. It also 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 time 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).

### 3.0 Conformance Standards Overview

The conformance standards are the central reference for organizations wanting to integrate their *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 allow 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.

#### 3.1 Common Volumes

The common volumes (Vol 1, Vol2, Vol 3A, Vol 4A and Glossary) 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 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*.

## 3.2 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 (in development)
- Volume 3D Business Rules – Provider Registry
- Volume 3E Business Rules – Provincial Lab Information Solution

### Volume 4 Application Enforced Rules and 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 for each ministry domain.

- Volume 4B Application Rules – Client Registry
- Volume 4C Application Rules – PharmaNet (in development)
- Volume 4D Application Rules – Provider Registry
- Volume 4E Application Rules – Provincial Lab Information Solution

## 3.3 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.

- **5A HIAL** - The HIAL enforces security and access policy; provides consent and disclosure management; and log and audit capability.
- **5B HNSecure** - HNSecure (inclusive of HNClient, HNServer/HNGate, HNGard) performs encryption/decryption, authentication and message routing services for organizations to securely exchange electronic health information via the Internet.

The conformance standards are available for download from the provincial website at <http://gov.bc.ca/healthinformationexchange>.

### 3.4 Required Conformance Standards by Service Integration

The following identifies the required Conformance Standards volumes for integration with 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	✓	✓	✓		✓			✓		✓		
Provider Registry	✓	✓	✓			✓		✓			✓	
Provincial Lab Information	✓	✓	✓				✓	✓				✓

Note: In addition, select the appropriate transport protocol (5A HIAL or 5B HNSecure).

### 3.5 Changes to the Conformance Standards

The following principles guide the development and publication of 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;
- The conformance standards are developed and published as a set of related volumes with a common release date and version; and
- The conformance standards contain only the rules for interfacing with ministry HIE services in British Columbia.

The conformance standards are published on the ministry website and will be republished as revisions are required. Release notes will be provided to indicate what portions of the conformance standards have changed.

Organizations can sign up for [conformance standards update notification services](#) through the provincial website to receive notifications of document updates. The ministry also provides [notification services for updates to user education materials](#) through the provincial website.

## 4.0 Integration Processes

The following table identifies the primary participants and a high level overview of their responsibilities throughout the integration and conformance processes. Please see the subsequent sections for more details regarding the integration process.

Table 2 Roles and Responsibilities

Role	Responsibility
Software Organizations (e.g., vendors, Health Authorities)	<ul style="list-style-type: none"> <li>• review the requirements for connecting to the ministry environments from the website <a href="http://gov.bc.ca/healthinformationexchange">http://gov.bc.ca/healthinformationexchange</a></li> <li>• download the conformance standards package</li> <li>• review the conformance standards applicable to your integration goal to understand the requirements</li> <li>• complete a '<a href="#">Request for Integration Services</a>' form and submit to Conformance and integration Services</li> <li>• participate in a vendor discovery session to review integration objectives and timelines with the ministry</li> <li>• sign a Vendor Participation Agreement with the ministry</li> <li>• contact Conformance and Integration Services to establish network connectivity</li> <li>• implement physical connections to provincial health networks</li> <li>• establish secure connection to ministry environments</li> <li>• complete endpoint, application and POS registration in required non-production and production environments</li> <li>• configure user ID's for non-production environments</li> <li>• conduct a self-assessment: a self-administered conformance readiness assessment to validate developed functionality prior to requesting a conformance test through the ministry</li> <li>• complete and submit a '<a href="#">Conformance Initiation Notice</a>' to request a conformance test through the ministry</li> <li>• incorporate ministry test data into POS application prior to the evaluation</li> <li>• demonstrate system conformance to the conformance standards through conformance evaluation</li> <li>• provide POS user support and training of certified</li> </ul>

Role	Responsibility
	<ul style="list-style-type: none"> <li>application to clients</li> <li>provide client support for user registration</li> </ul>
Ministry Conformance and Integration Services Team	<ul style="list-style-type: none"> <li>publish the conformance standards and education material</li> <li>facilitate/coordinate network connectivity</li> <li>facilitate/coordinate connectivity to various ministry environments</li> <li>receive and facilitate responses to software organizations' questions and issues</li> <li>provide test cases and test data required for development, conformance evaluation and training needs</li> <li>coordinate and oversee the conformance evaluation sessions</li> <li>prepare the conformance evaluation report</li> <li>issue conformance certification</li> <li>maintain a registry of certified products</li> </ul>
Ministry Domain Evaluation Team(s)	<ul style="list-style-type: none"> <li>prepare test cases and test data</li> <li>validate transactions against a set of test cases and expected results</li> <li>evaluate each tested requirement (pass or fail)</li> <li>sign/approve final outcome of conformance test</li> </ul>

#### 4.1 Apply for Integration Services

The ministry assists software organizations interested in integrating with HIE services. Software organizations must first understand the requirements for integration by reviewing the integration options, conformance standards and legal agreement.

Subsequent to their review, the software organization completes a 'Request for Integration Services' form available on the [Forms](#) section of our website and submits it to the ministry at [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca).

The ministry then hosts discovery sessions with the organization to ensure the latter's integration plans align with the ministry business strategy, to verify their understanding of the requirements, to identify any constraining factors and to determine the appropriate integration approach.

The goal of these sessions is for the ministry and the organization to reach a consensus view on whether the time is right to proceed with the integration plan.

Questions related to the conformance process, conformance standards or software organization requirements are to be submitted to the ministry at [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca).

## 4.2 Register for Ministry System Access

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

### 4.2.1 Ministry Service Access Prerequisites

#### 4.2.1.1 Software Organizations

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

- follow the registration and engagement processes outlined in the integration process (Vol 1);
- sign a Vendor Participation Agreement prior to environment access;
- develop software that implements the application enforced rules provided in the Application Enforced Rules (Vol 4);
- implement the technical mechanisms to connect to ministry systems as provided in the Message Specifications (Vol 5 Specs);
- initiate and complete the conformance process;
- adhere to privacy and security obligations (Vol 2); and
- ensure users comply with the general and domain specific business rules (Vol 3).

#### 4.2.1.2 Points 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.

In order to use their POS application to access ministry HIE services, POS organizations and users must:

- follow the registration processes and adhere to the business rules in Volume 3 - Business Rules;
- sign a data access agreement; and
- receive appropriate training.

## 4.2.2 Environment Access Prerequisites

### 4.2.2.1 Medical Practice Applications

Software organizations providing medical practice applications, often referred to as *electronic medical record applications (EMR)*, must provide an *Application Service Provider (ASP)* hosted solution. Medical Practice POS applications that are not hosted by an ASP are not permitted to connect to ministry health information systems. An ASP provides network-based access to application services, which involves:

- remotely hosting a client's EMR system, application and data on its secured computer servers;
- providing client access through a web browser or thin client;
- professionally managing the servers and other related technologies on the client's behalf; and
- ensuring no server hardware or software is present at the point of care.

To fully protect patient privacy and confidentiality and provide high quality service delivery the:

- ASP solution must be hosted in a secure, centralized, and professionally managed data centre, located in an environmentally safe location (i.e., away from potential earthquake, flood, and fire zones);
- data centre must have sufficient physical infrastructure for providing high quality service, including: heating, ventilation, air conditioning ('HVAC') controls, fire suppression controls, and an uninterruptible power supply;
- data centre must meet the security requirements outlined in volume 2 of the conformance standards; and
- ASP solution must acquire and provision software service delivery over a dedicated circuit between the data centre and the provincial Extranet which is an aggregation and access point for public sector health.

### 4.2.2.2 Sandbox Environment Access

The sandbox environment is available for software organizations to complete their integration development. Software organizations must complete the following activities before the ministry can grant access to the sandbox environment:

- review complete set of Conformance Standards and associated message specifications;
- subscribe to vendor notifications to receive changes to the conformance standards;
- understand and commit to what is required for full integration with ministry systems;
- procure a dedicated network circuit and establish required routing when using the HIAL;
- complete and submit the Request for Integration Services form (see Appendix B);
- sign an appropriate vendor participation agreement;
- configure their system for sandbox environment connectivity:
  - register endpoints, application and a point-of-service
  - register test user IDs
  - perform smoke testing; and
- agree to appropriate sandbox environment usage.

#### 4.2.2.3 Conformance Environment Access

The conformance environment is used by software organizations to demonstrate their compliance to the conformance standards. Prior to access being granted to the conformance environment, software organizations must:

- conduct a conformance self-test to validate conformance to the conformance standards;  
Note: A conformance self-test must be conducted in the sandbox environment to confirm the ability to pass all rules as specified in the conformance standards prior to requesting a formal ministry conformance test
- complete and submit a 'Conformance Initiation Notice' (Appendix B) to request a formal conformance test;
- agree to appropriate conformance environment usage; and
- configure system for conformance environment connectivity:
  - register endpoints, application and a point-of-service;
  - register test user IDs; and
  - perform smoke testing.

#### 4.2.2.4 Training and Production Environment Access

The training environment is used to conduct end user training exercises. Furthermore, it can be accessed by end users on an ongoing basis to refresh their understanding of and practice using ministry HIE services. Prior to gaining access to either the training or production environments, software organizations must:

- Receive certification from the ministry
- Confirm their vendor registration information and provide a privacy contact
- Configure system for training environment connectivity:
  - to prepare for client use;
  - register endpoints, application and points-of-service;
  - register training user IDs; and
  - perform smoke testing.
- Configure system for production environment connectivity:
  - register endpoints, application and points-of-service; and
  - perform smoke testing.
- Understand and use the ministry's user/vendor support model

### 4.2.3 Software Organization

The ministry's Conformance and Integration Services 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 in order to start the process of integration. The ministry will be the point of contact for each of the items described in this section and can be contacted at [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca).

The applicability of each of the following registration forms will depend on the organization's type of system and current and desired HIE service access. Software organizations providing medical practice applications and health authorities use the *Health Information Access Layer (HIAL)* while others may be required to use HNSecure to connect points of service to the ministry's legacy systems via the Internet.

#### 4.2.3.1 HIAL Registration

Registration for the HIAL requires configuration information and a Certificate Signing Request (described below). At this time, community pharmacy POS are not required to access PharmaNet through the HIAL. Communication with the HIAL is protected by mutually authenticated HTTPS protocol, requiring certificates to be exchanged and authenticated by both client and server systems.

To enable mutual authentication, software organizations must generate a digital certificate, have it signed by HIAL administration and configure the POS endpoint to present the signed certificate during HTTPS session negotiation. Detailed instructions are provided in Conformance Standards Volume 5A - Transport Protocols - Health Information Access Layer (HIAL).

#### 4.2.3.2 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 conformance standards Volume 5B – HNSecure.

#### 4.2.4 POS User Registration

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

##### 4.2.4.1 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).

##### 4.2.4.2 Medical Practice (EMR)

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 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.

#### 4.2.4.3 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, Information Support at Health Insurance BC (HIBC) can initiate the PharmaNet connection process. All subsequent inquiries will be handled through HIBC.

### 4.3 Evaluation and Compliance

#### 4.3.1 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 compliance evaluation.

Compliance evaluations will:

- facilitate a fair and consistent evaluation of all software organizations' applications and processes; and
- assess whether or not 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 compliance is established through attestation or submission of supporting documentation as well as demonstrable standards in a formal evaluation session.

#### 4.3.2 Scheduling

Software organizations must complete and submit a ministry provided 'Conformance Initiation Notice'. The application form is available for download from the [Forms page](#) on the provincial website. 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. 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.

### 4.3.3 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 test the conformance rules, but may not reflect standard workflow. Organizations will be required to complete and pass all provided test cases as well as message verification.

Test cases and data are available from the ministry at [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca)

### 4.3.4 Evaluation

Conformance standards 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; and demonstrating compliance to the stated standards;
- message level validation; and
- submission of training plans and materials.

Questions regarding the conformance evaluation process must be directed to the ministry at [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca)

### 4.3.5 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.

### 4.3.6 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.

In the event that 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.

#### **4.3.7 Evaluation Results**

During the conformance test ministry representatives will document the results of each test and provide feedback.

#### **4.3.8 Compliance**

A formal letter of compliance will be issued upon successful completion of the conformance test.

#### **4.3.9 Non-Compliant Results**

Should the software organization not successfully pass the conformance test they will be given a report of the specific rules failed during the test.

## 5.0 Agreements

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

### 5.1 Circuit Orders and Connection Agreements (for HIAL access only)

Access to HIAL services requires physical connection to health networks and creation of network paths from the software organization's environments to corresponding HIAL environments.

Physical connections require a circuit between the software organization's physical site and the Health Extranet. The Extranet network is managed by the BC Clinical and Support Services (BCCSS) on behalf of the ministry. If not already in place, this circuit must be ordered through HSSBC. Circuit orders require agreements and signatures by the connecting parties. Network addresses will be assigned during this installation. If the software organization's development and production sites differ, the organization may need to consider two circuits.

For each environment (sandbox, conformance, training and production), a logical path between the software organization's site(s) and the HIAL must be established.

### 5.2 Vendor Participation Agreement

Software organizations must sign a Vendor Participation Agreement prior to being granted access to ministry environments. The signing of the agreement may be conducted concurrently with the initial onboarding process. Software organizations should consult their own legal counsel for any questions with respect to the agreement.

### 5.3 Information Sharing Agreements - Health Authorities

Health authorities generally have information sharing agreements in place that will cover the obligations for their software integration with ministry HIE services. For further details regarding these agreements, please contact the ministry at [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca)

## 6.0 Tools for Software Organizations

### 6.1 EMR Reference Implementation

The ministry's Electronic Medical Record (EMR) reference implementation (RI), an example of medical practice EMR software integrated with ministry systems through the HIAL, is available to assist registered EMR software organizations with their interface development. Its use is optional.

It is based on Java technologies with 2 major architectural components:

- HIAL Bridge: implements sending and receiving messages to and from the BC HIAL; plug-in packages are available for each of the following services: Client Registry, Provider Registry, PharmaNet and Provincial Laboratory Information Solution.
- miniEMR: a web-based EMR simulator that illustrates the details associated with typical workflows for an EMR.

The source code can be used as is or studied for implementing an organization's own solution:

- The code can be used as a sample code reference to understand coding options in integrating with the EHR;
- code can be re-used directly (embedded) when customizing an EMR solution; and
- The RI can be installed on the software organization's server, and once the software organization has connected with the ministry systems, the application can be run for various scenarios to understand a possible implementation.

Use of the RI may reduce risk, reduce cost, and accelerate implementation. The RI software and technical documentation is made available under the Apache Version 2.0 license and GNU General Public License. This is a conventional license that enables software organizations to utilize the software and documentation in open or closed source applications with no royalties or costs.

The RI is available upon request to [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca).

### 6.2 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.

## 7.0 Non-Production Environment Data

### 7.1 Overview

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, PR, 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 and conducting a conformance self-test to validate compliance to the conformance standards. 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 that their application complies with all the requirements specified in the Conformance Standards.
- **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 in the Volume 3 set. For any organization-specific requirements for training data, see below.

### 7.2 Types of Data

#### 7.2.1 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.

##### 7.2.1.1 Types of Shared Data

**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, PR 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.

## 7.2.2 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.

### 7.2.2.1 Identifying Organization-Specific Data

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.

### 7.2.2.2 Requesting Organization-Specific Data

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

Organization Type	Repository	Contact
EMR Software Organizations	PharmaNet Client Registry Provider Registry Provincial Laboratory Information Solution	HLTH.CISSupport@gov.bc.ca
Health Authority organizations using the HIAL	PharmaNet Client Registry Provider Registry Provincial Laboratory Information Solution	HLTH.CISSupport@gov.bc.ca
Health Authority organizations NOT using the HIAL (e.g., using the Registry Broker)	Client Registry Provider Registry	VSA.REGISTRIESADMIN@gov.bc.ca
Health Authority organizations NOT using the HIAL	PharmaNet	HLTH.CISSupport@gov.bc.ca
Pharmacy Software organizations	PharmaNet	pcaresupport@maximusbc.ca

## 7.2.3 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').

### 7.3 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:

Repository	View Methodology
Client Registry	Use organization's application to issue query and view data Use Client Registry web application
Provider Registry	Use Provider Registry web application
PharmaNet	Use organization's application to issue query and view data
PLIS	Use organization's application to issue query and view data

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

- applicable registry (Client or Provider),
- full name of the user(s),
- each user's email address, contact information and role.

### 7.4 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 has to 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 email to VSA.REGISTRIESADMIN@gov.bc.ca
Provider Registry	Generate a distribution	Send email to VSA.REGISTRIESADMIN@gov.bc.ca
PharmaNet	Dispense a sample	Issue the Medication Update – TMU (01 / 51) transaction
	Reverse a sample dispense	Issue the Medication Update Reversal – TMU (11 / 61) transaction

Repository	Desired Result	Software Organization Action
	Dispense a prescription on a non-sample medication Adapt a prescription Reverse a dispense issued on a non-sample medication	Send email to <a href="mailto:pcaresupport@maximusbc.ca">pcaresupport@maximusbc.ca</a>
PLIS	Update or correct a lab record Withdraw a report	Send email to <a href="mailto:HLTH.CISSupport@gov.bc.ca">HLTH.CISSupport@gov.bc.ca</a> to have 'Day 2' lab data loaded
	Set a corrected or updated lab record back to its initial state Set a withdrawn report back to its initial state	Send email to <a href="mailto:HLTH.CISSupport@gov.bc.ca">HLTH.CISSupport@gov.bc.ca</a> to have 'Day 1' lab data loaded

## 7.5 Environment Data Refresh

### 7.5.1 Sandbox Environment

The **Client Registry and Provider Registry 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 **PharmaNet sandbox** environment is refreshed nightly to ensure that 'production like' personal information is not introduced into the environment. It is important to note that as a result of this process the data in organization's application-based data (local system ) and the ministry repository data will not be synchronized.

Integrated data (PHNs exist in other domains) and shared data sets are excluded from the nightly cleanse as these data sets are expected to be Read-Only.

For details related to specific data fields affected please contact: [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca)

The **PLIS environment** can be refreshed to either 'Day 1' or 'Day 2' scenario data, upon request of a software organization. To have the PLIS environment set to the desired dataset, contact the ministry at: [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca).

Questions related to data in all non-production environments should be directed to: [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca)

### 7.5.2 Conformance Environment

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

### 7.5.3 Training Environment

The Client Registry and Provider Registry 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. To have the PLIS environment set to the desired dataset, contact the ministry at: [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca)

The PharmaNet training environment is refreshed nightly; therefore, software organizations are encouraged to refresh their local (application-based) corresponding clinical data nightly to ensure the local data and the ministry repository data remain synchronized. Software organizations may request that certain data be added permanently to the nightly PharmaNet training baseline; contact [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca) if this is desired.

## 7.6 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.

## 8.0 Support Model

### 8.1 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.

All ministry contact is to be directed to: [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca)

### 8.2 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)	<ul style="list-style-type: none"> <li>If not provided by the software organization, advise the user to contact their IT support.</li> </ul>						
POS application	<ul style="list-style-type: none"> <li>open an internal “ticket” and resolve the incident through your own support organization;</li> <li>advise users; and</li> <li>close the ticket.</li> </ul>						
Network (PPN, VPN)	<ul style="list-style-type: none"> <li>open a “ticket” with the Tier 2 support organization (TELUS);</li> <li>monitor the progress of the resolution and, if required, escalate;</li> <li>contact the originator of the call to confirm the incident was resolved to their satisfaction; and</li> <li>close the ticket with the Tier 2 support organization.</li> </ul>						
HIAL	<ul style="list-style-type: none"> <li>open a “ticket” with the Tier 2 support organization (EHealth Operations Service Desk 604-675-4299 or <a href="mailto:servicedesk@phsa.ca">servicedesk@phsa.ca</a>); NOTE: indicate ticket is to be assigned to VPP-eHealth Technical</li> <li>monitor the progress of the resolution and, if required, escalate;</li> <li>contact the originator of the call to confirm the incident was resolved to their satisfaction; and</li> <li>close the ticket with the Tier 2 support organization.</li> </ul>						
HNSecure	<ul style="list-style-type: none"> <li>open a “ticket” with the Tier 2 support organization; <ul style="list-style-type: none"> <li>(ministry Help Desk 250-952-1234 or <a href="mailto:HLTH.Helpdesk@gov.bc.ca">HLTH.Helpdesk@gov.bc.ca</a> )</li> </ul> </li> <li>monitor the progress of the resolution and, if required, escalate;</li> <li>contact the originator of the call to confirm the incident was resolved to their satisfaction; and</li> <li>close the ticket with the Tier 2 support organization.</li> </ul>						
Business or data incident	<p>Contact the appropriate Tier 2 support organization on the user’s behalf.</p> <table border="1"> <tbody> <tr> <td>PharmaNet</td> <td>1-800-554-0225 (toll free) 604-682-7120 (Vancouver)</td> </tr> <tr> <td>Registries</td> <td>250-952-9137 <a href="mailto:VSA.REGISTRIESADMIN@gov.bc.ca">VSA.REGISTRIESADMIN@gov.bc.ca</a></td> </tr> <tr> <td>PLIS</td> <td>604-675-4299 <a href="mailto:servicedesk@phsa.ca">servicedesk@phsa.ca</a></td> </tr> </tbody> </table>	PharmaNet	1-800-554-0225 (toll free) 604-682-7120 (Vancouver)	Registries	250-952-9137 <a href="mailto:VSA.REGISTRIESADMIN@gov.bc.ca">VSA.REGISTRIESADMIN@gov.bc.ca</a>	PLIS	604-675-4299 <a href="mailto:servicedesk@phsa.ca">servicedesk@phsa.ca</a>
PharmaNet	1-800-554-0225 (toll free) 604-682-7120 (Vancouver)						
Registries	250-952-9137 <a href="mailto:VSA.REGISTRIESADMIN@gov.bc.ca">VSA.REGISTRIESADMIN@gov.bc.ca</a>						
PLIS	604-675-4299 <a href="mailto:servicedesk@phsa.ca">servicedesk@phsa.ca</a>						

Origin or Incident	Action		
			NOTE: indicate ticket is to be assigned to 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:

System	Schedule	Day	Time
PharmaNet	Weekly	Thursday	12:00 am – 8:00 am
	Weekly	Sunday	1:00 am – 5:00 am
Client Registry	Weekly	Sunday	1:00 am – 5:00 am
Provincial Lab Information Solution	Weekly	Sunday	2:00 am – 4:00 am
	Monthly	2nd Wednesday	6:00 am – 8:00 am
Provider Registry	Weekly	Thursday	12:00 am – 6:00 am
		Sunday	12:00 am – 6:00 am

### 8.3.2 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.

## 8.4 Non-Production Environments

### 8.4.1 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 – training environment	Weekly	Sunday, Monday, Wednesday, Friday	2am to 3am
PharmaNet – training environment	Weekly	Tuesday and Thursday	2am to 9am <sup>1</sup>
PharmaNet – sandbox and conformance environment	N/A <sup>2</sup>	N/A <sup>2</sup>	N/A <sup>2</sup>
Client Registry	Weekly	Sunday	12:00 am – 6:00 am
Provincial Lab Information Solution	N/A <sup>3</sup>	N/A <sup>3</sup>	N/A <sup>3</sup>
Provider Registry	Weekly	Sunday and Thursday	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.

### 8.4.2 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.

## 9.0 Continued Conformance

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
- Reduce the risk of data integrity or system availability issues arising in production.

### 9.1 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.

### 9.2 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.

### 9.3 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.

### 9.4 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.

### 9.5 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 wait for ministry approval prior to implementing the new release in a production environment. Complete the '[Application Release Assessment](#)' form and submit it to [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca). The ministry response to the submission can be expected within 7 business days of the form's submission.

### **9.5.1 POS Application Emergency Upgrades**

Emergency changes made to certified POS applications must be reported to the ministry by the following working day.

Complete section 4.0 of the "Application Release Assessment" form and submit it to [HLTH.CISSupport@gov.bc.ca](mailto:HLTH.CISSupport@gov.bc.ca).

## 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	
<input type="checkbox"/>	Contact Conformance and Integration Services with any questions regarding the conformance standards (rules or specifications), network issues or general questions regarding readiness.
Conformance Self-test	
<input type="checkbox"/>	Run a self-test in the sandbox environment using the provided test plan (if available) to confirm the application passes the rules specified in the Conformance Standards. Do this prior to requesting a formal ministry conformance test.
Conformance Test Request	
<input type="checkbox"/>	Submit a Conformance Initiation Notice to Conformance and Integration Services to schedule a formal conformance test.
Environment Readiness	
	For applications using the HIAL:
<input type="checkbox"/>	Confirm that you have registered, supplied your configuration information and setup a secured connection (certificate signing process) to the conformance environment.
<input type="checkbox"/>	Confirm you have the user IDs to access the conformance environment (these will differ from the ones used in the sandbox environment).
	For applications using HNSecure:
<input type="checkbox"/>	Confirm you have registered for and received the facility ID to be used for the evaluation. These are different from those used during development.
Test Data	
<input type="checkbox"/>	Receive and add test data to the POS application prior to the evaluation.
Evaluation Location and Facilities	
<input type="checkbox"/>	Understand the remote facilities and tools to be used for conducting the evaluation remotely (unless an on-site evaluation is requested). 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:
<input type="checkbox"/>	Is knowledgeable of the software product and the test cases
<input type="checkbox"/>	Is able to perform and display all required functions
<input type="checkbox"/>	Has the ability to provide screen shots upon request
<input type="checkbox"/>	Has access to technical support if required
<input type="checkbox"/>	Is available throughout the scheduled testing cycle

## Appendix B: Forms

The forms referenced in this document can be downloaded from [Forms page](#) on the provincial website.

Form File Name
Request for Integration Services (Form#: HLTH 4637)
Conformance Initiation Notice (Form#: HLTH 4636)
HNSecure Registration - Specific To Pharmacy Access To PharmaNet
Application Release Assessment