BRITISH COLUMBIA
Ministry of Health

British Columbia
Professional and Software Conformance Standards

Electronic Health Information Exchange

Volume 2: Software Organization Processes

Version 1.2.3   2015-12-21

Security Classification: Low Sensitivity

Copyright Notice

Disclaimer and Limitation of Liabilities

This document and all of the information it contains is provided "as is" without warranty of any kind, whether express or implied. All implied warranties, including, without limitation, implied warranties of merchantability, fitness for a particular purpose, and non-infringement, are hereby expressly disclaimed.

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

Author:	MoH Conformance Services
Date Created:	2011-01-05
Last Updated:	2015-12-21
Version:	1.2.3

Table of Contents

Tables

1.0 Introduction

Software 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 Conformance Standards Volume Set

The Conformance Standards are the central reference for organizations wanting to integrate their *Point of Service (POS)* applications with ministry HIE services. This integration will allow their 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 volumes in the Conformance Standards are divided into topics such as: business rules, application-enforced rules, change management rules, privacy and security rules, and technical message and transport specifications. The Conformance Standards are available on the Conformance and Integration Services website:
http://gov.bc.ca/healthinformationexchange

1.2 Key to Document Terminology

The Conformance Standards in this volume use a consistent language convention:

- The word "should" is used to indicate a recommended requirement meaning that the standard is optional (i.e., not compulsory yet encouraged). Conformance testing, service on-boarding activities and/ or application testing will confirm that this standard is correctly implemented where appropriate.
- All other standards or rules as stated are a compulsory function or requirement. The words "must" "will", "minimum", or "mandatory" are used to indicate this. 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.

1.3 Purpose of Document

This document describes the integration and conformance processes and requirements for software organizations integrating with ministry HIE services, including:

- Roles and responsibilities
- Integration prerequisites
- Registration and agreements
- Tools
- Evaluation and certification
- Support model
- POS application management

1.4 Intended Audience

The intended audience for this document is:

- **Software Organizations** – organizations (including in-house system development teams) who develop interfaces to HIE services and/or support those interfaces;
- **Conformance Team(s)** – who are responsible for evaluating and testing conformance, including organizational security practices and business processes; and
- **Audit Team(s)** – who are responsible for independent examination and evaluation of compliance including organizational security practices and business processes.

1.5 Ministry of Health Conformance Standards Contact

Questions regarding the Conformance Standards should be directed to Conformance and Integration Services at: HLTH.CISSupport@gov.bc.ca

2.0 Roles and Responsibilities

The following table identifies the primary participants and their responsibilities throughout the integration and conformance processes.

Table 1 Roles and Responsibilities

Role	Responsibility
Software Organizations (e.g., vendors, Health Authorities)	• Go to the software development standards site: www.health.gov.bc.ca/access/software_development.html ○ Download the Conformance Standards package from the website ○ Review the Conformance Standards to understand the requirements ○ From the website, review the requirements for connecting to the ministry environments • Sign an Information Sharing Agreement or Vendor Participation Agreement with the ministry • Contact Conformance and Integration Services to establish network connectivity • Implement physical connections to provincial health networks • Establish secure connection to ministry environments • Complete endpoint, application and POS registration in required non-production and production environments • Configure user IDS for non-production environments • Conduct a *self-assessment* - a self-administered conformance readiness assessment to validate developed functionality prior to requesting a conformance test through the ministry • Complete and submit a ‘Conformance Initiation Notice’ to request a conformance test through the ministry • Incorporate ministry test data into POS application prior to the evaluation • Demonstrate system conformance to the Conformance Standards through conformance evaluation • Provide POS user support and training of certified application to clients • Provide client support for user registration
Ministry Conformance and Integration Services Team	• Publish the Conformance Standards and education material • Facilitate/coordinate network connectivity • Facilitate/coordinate connectivity to various ministry environments • Receive and facilitate responses to software organizations’ questions and issues

Role	Responsibility
	• Provide test cases and test data required for development, conformance evaluation and training needs • Coordinate and oversee the conformance evaluation sessions • Prepare the conformance evaluation report • Issue conformance certification • Maintain a registry of certified products
Ministry Domain Evaluation Team(s)	• Prepare test cases and test data • Validate transactions against a set of test cases and expected results • Evaluate each tested requirement (pass or fail) • Sign/approve final outcome of conformance test

3.0 How to Apply for Conformance and Integration Services

The ministry encourages and 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 Forms section of our website and submits it to the ministry at 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 initiative.

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.

4.0 Environment Access Prerequisites

4.1 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.
- No server hardware or software required 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.)
- The 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.
- The data centre must meet the security requirements outlined in Volume 9 of the conformance standards, which includes, but is not limited to, physical and logical security measures such as:
    - Physical and environmental security measures including:
        - Strong physical security perimeters, alarmed fire doors, and armoured windows;
        - Entry and exit logs;
        - Locks activated by keypads, swipe cards or equivalent;
        - Intruder alarms;
        - Security guards; and
    - Recorded video surveillance. Commercial-grade firewalls and intrusion/detection systems.
    - System monitoring and auditing for unauthorized access.
- The ASP solution must acquire and provision software service delivery over a dedicated TELUS circuit between the data centre and the provincial Extranet which is an aggregation and access point for public sector health.

4.2 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:

1. Review complete set of Conformance Standards and associated message specifications
2. Subscribe to vendor notifications to receive changes to the Conformance Standards
3. Understand and commit to what is required for full integration with ministry systems
4. When using the HIAL, procure a dedicated network circuit and establish required routing
5. Complete and submit the Vendor Application for CIS Services (see Appendix B)
6. Sign a data sharing agreement (for health authorities) or a vendor participation agreement (for private vendor organizations)
7. Configure their system for sandbox environment connectivity:
    - register endpoints, application and a point-of-service
    - register test user IDs
    - perform smoke testing
8. Agree to appropriate sandbox environment usage

4.3 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:

1. 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.

2. Complete and submit a 'Conformance Initiation Notice' (Appendix B) to request a formal conformance test
3. Agree to appropriate conformance environment usage
4. Configure system for conformance environment connectivity:
    - register endpoints, application and a point-of-service
    - register test user IDs
    - perform smoke testing

4.4 Training and Production Environment Access

The training environment is used by software organizations 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:

1. Pass conformance tests for:
    - privacy and security Conformance Standards
    - domain-specific application-enforced Conformance Standards
    - change management and training Conformance Standards

    - message-specific conformance tests

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

5.0 Registration for Ministry System Access

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

5.1 Software Organization

5.1.1 General

The ministry's Conformance and Integration Services 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.

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.

5.1.2 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).

5.1.3 HNSecure Registration

HNSecure is legacy 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 – Transport Protocols – HNSecure.

5.2 POS User Registration

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

5.2.1 Health Authority

The registration of health authority users accessing the ministry information exchange 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).

5.2.2 Medical Practice

The medical practice 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.

5.2.3 Pharmacy

The pharmacy’s initial enquiries 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 enquiries will be handled through HIBC.

6.0 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.

6.1.1 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 Health Shared Services (HSSBC) for the ministry. If not already in place, this circuit must be ordered through HSSBC and installed by TELUS. 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.

6.1.2 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.

6.1.3 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. This will be confirmed during the Privacy Impact Assessment (PIA) and Security Threat and Rick Assessment (STRA) processes that they will undergo to verify their compliance to privacy and security conformance standards.

7.0 Tools for Software Organizations

7.1 EMR Reference Implementation (RI)

The 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.
- The code can be re-used directly (embedded) when customizing an EMR solution.
- 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.

7.2 HNSecure Toolkit

HNSecure is legacy 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.

7.3 PharmaNet Reference Model API

The PharmaNet API Guide is a standard API between POS applications and PharmaNet and provided as a resource for software developers. Use of the PharmaNet API Guide is optional. Software organizations can use the sample API software directly or as a template for their own development. It consists of a driver program, a mainline API, data compression and expansion modules, plus various routines to perform DES-based encryption and decryption of message segments.

The software and further information is available by contacting the Conformance and Integration Services at HLTH.CISSupport@gov.bc.ca

8.0 Change Notifications

Software organizations that have subscribed through the ministry website subscription service will receive automated notifications of any updates and new releases to the Conformance Standards.

All new releases of the Conformance Standards will be made available on the following website: http://gov.bc.ca/healthinformationexchange

Subscribe for notification of changes to the Conformance Standards from the Conformance Standards page on the provincial website.

Subscribe for notification of changes to the user education materials from the User Reference Information page on the provincial website.

9.0 Non-Production Environment Data

9.1 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 (Client Registry, Provider Registry, 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 Volumes 4 and 4X. For any organization-specific requirements for data, see below.
- **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 for software organizations to demonstrate their 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 Volumes 6 and 6x. For any organization-specific requirements for training data, see below.

9.2 Test Plans

Once a software organization has completed its application interface development, they need to perform a conformance self-test in the sandbox environment to validate the application meets all conformance standards.

Test plans have been developed to support this validation exercise. Scenarios encompassing the conformance standards on which the software organization will be tested are included in the test plan. The data to support each scenario is specifically identified. By using the specified data, the organization will be able to validate that its application generates the expected results anticipated in the conformance test.

9.3 Types of Data

9.3.1 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.

9.3.1.1 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 (Client Registry, PharmaNet, Provider Registry and the Provincial Laboratory Information Solution) 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 Client Registry, they are best used for the clinical domain transactions only.

9.3.2 Identifying Shared Data

All shared data will be identified by the '*usage identifier*' that is prepended to the patient's last name. The table below depicts the usage identifier for shared data in the sandbox and training environments.

SHARED DATA – SANDBOX ENVIRONMENT					
Client Registry UI: S e.g., SSmith	**PharmaNet UI: ___**	**PLIS UI: EH e.g., EHSmith**	**Provider Registry UI: ___**		**Integrated Data (CR, PNET, PLIS, PR)**
					PHNs UI: EH e.g., EHSmith
SHARED DATA – TRAINING ENVIRONMENT					
Client Registry UI: T e.g., TSmith	**PharmaNet UI: TR e.g., TRSmith**	**PLIS UI: EH e.g., EHSmith**	**Provider Registry UI: ___**		**Integrated Data (CR, PNET, PLIS, PR)**
					PHNs UI: EH e.g., EHSmith

9.3.3 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.

9.3.3.1 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.

9.3.3.2 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
Pharmacy Software organizations	PharmaNet	pcaresupport@maximusbc.ca

9.3.4 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'.)

9.4 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

Repository	View Methodology
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.

9.5 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
	• Dispense a prescription on a non-sample medication • Adapt a prescription • Reverse a dispense issued on a non-sample medication	Send email to pcaresupport@maximusbc.ca

Repository	Desired Result	Software Organization Action
PLIS	Update or correct a lab record Withdraw a report	Send email to HLTH.CISSupport@gov.bc.ca 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 HLTH.CISSupport@gov.bc.ca to have 'Day 1' lab data loaded

9.6 Environment Data Refresh

9.6.1 Sandbox Environment

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

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

9.6.2 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.

9.6.3 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

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 if this is desired.

9.7 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.

10.0 Conformance Evaluation and Certification

10.1 Overview

To access the ministry HIE services the POS systems must comply with the HL7 messaging specifications and the defined Conformance Standards. The POS system must pass the provincial conformance evaluation and certification process.

Conformance evaluations will:

- Facilitate a fair and consistent evaluation of all software organizations' applications and processes.
- Assess whether or not the POS application:
  - properly implements the standards and technical specifications;
  - provides accurate and correctly interpreted data;
  - operates efficiently with the integrated systems.

Evidence of conformance is established through:

- **Volume 4 POS Application Enforced Rules** – This volume contains the rules that are to be enforced by the POS application. Demonstration of conformance is through a formal conformance session (described later in this document).
  - Allow 3-5 days for testing for each HIE service (e.g., Client Registry, PharmaNet, PLIS) being implemented. Remediation will require a full regression test.
- **Volume 4 Supplement** – this package contains the technical specifications for message interactions, message construction and markup rules.
  - inspection for adherence to the message specifications will be part of the formal conformance session
  - software organizations will be expected to submit their own logs detailing message throughput to the ministry HIE services as part of the conformance session.
- **Volume 5 Transport Protocols** - The technical mechanisms by which POS systems access and exchange messages with ministry systems. Transmission of messages will be reviewed as part of the formal conformance session.
- **Volume 6 Change Management** - Training and Education – Compliance to the Conformance Standards in Volume 6 is demonstrated through a combination of attestation and submission of identified supporting documentation.
- **Volumes 7 and 8 Privacy and Security** (health authority systems) - The rules identified in these volumes must be demonstrated through attestation or submission of supporting documentation. Demonstrable standards are covered through the Privacy Impact Assessment (PIA) and Security Threat Risk Assessment (STRA) processes.

- **Volume 9 Privacy and Security** (all organizations) - The rules identified in these volumes must be demonstrated through attestation or submission of supporting documentation as well as demonstrable standards in a formal conformance session.

10.2 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.

Note that a four week 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.

10.3 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. You 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

10.4 Evaluation

Evaluation sessions may take 5 or more days depending on the HIE service being tested. Sessions will take place on consecutive days during normal business hours, Monday through Friday.

All evaluation sessions will be done remotely (e.g., using LiveMeeting or Link) unless the software organization requests to attend in person at a Victoria location and pre-arrangements are made. Travel expenses associated with conformance evaluation will be at the software organization's expense.

The application will be evaluated against the expected results of each test case and the transmission of transactions to the ministry conformance environment. The evaluation team will assess the results of test cases and assign a 'pass' or 'fail' to each rule within the test case and, after the conformance test, verify the messages through schema validation, schematron validation or a combination.

If the application fails to perform as required, the evaluation team will determine the extent of the failure and/or if it is clear the application is not conformance ready. If it is determined the organization is not ready for conformance, the testing session will be stopped and the organization will have to submit another Conformance Initiation Notice to schedule a regression test.

Questions regarding the conformance evaluation process must be directed to the ministry at HLTH.CISSupport@gov.bc.ca

10.5 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.

10.6 Test Scoring

A 'pass' or 'fail' will be assigned to the result of each test case based on the following Scoring Criteria Table:

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 (i.e., 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.

10.7 Evaluation Results

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

10.7.1 Certification

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

10.7.2 Non-conformant 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.

11.0 Support Model

11.1 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

11.2 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 EHR Services; and
- Managing and closing incidents with the users.

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

Origin or Incident	**Action**
Client hardware, software, network infrastructure, or security software (firewall, antivirus)	If not provided by the software organization, advise the user to contact their IT support.
POS application	1. Open an internal “ticket” and resolve the incident through your own support organization, 2. Advise users, and 3. Close the ticket

<table>
<tr><th>Origin or Incident</th><th>Action</th></tr>
<tr><td>Network (PPN, VPN)</td><td>1. Open a “ticket” with the Tier 2 support organization (TELUS),
2. Monitor the progress of the resolution and, if required, escalate,
3. Contact the originator of the call to confirm the incident was resolved to their satisfaction,
4. Close the ticket with the Tier 2 support organization.</td></tr>
<tr><td>HIAL</td><td>1. Open a “ticket” with the Tier 2 support organization (EHealth Operations Service Desk 604-675-4299 or servicedesk@phsa.ca)
NOTE: indicate ticket is to be assigned to VPP-eHealth Technical
2. Monitor the progress of the resolution and, if required, escalate,
3. Contact the originator of the call to confirm the incident was resolved to their satisfaction, and
4. Close the ticket with the Tier 2 support organization.</td></tr>
<tr><td>HNSecure</td><td>1. Open a “ticket” with the Tier 2 support organization (ministry Help Desk 250-952-1234 or HLTH.Helpdesk@gov.bc.ca)
2. Monitor the progress of the resolution and, if required, escalate,
3. Contact the originator of the call to confirm the incident was resolved to their satisfaction, and
4. Close the ticket with the Tier 2 support organization.</td></tr>
<tr><td>Business or data incident</td><td>1. Contact the appropriate Tier 2 support organization on the user’s behalf.
<table>
<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
VSA.REGISTRIESADMIN@gov.bc.ca</td></tr>
<tr><td>PLIS</td><td>604-675-4299
servicedesk@phsa.ca
NOTE: indicate ticket is to be assigned to VPP-eHealth Technical</td></tr>
</table></td></tr>
</table>

11.3 Service Interruption - Production Environment

11.3.1 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

11.3.2 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.

11.4 Non-Production Environments

11.4.1 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
Medication Information	PharmaNet – training environment	Weekly	Sunday, Monday, Wednesday, Friday	2am to 3am
	PharmaNet – training environment	Weekly	Tuesday and Thursday	2am to 9am*
Patient Demographic Information	Client Registry	Weekly	Sunday	12:00 am – 6:00 am
Patient Lab Information	Provincial Lab Information Solution	N/A	N/A	N/A
Health Care Provider Demographic Information	Provider Registry	Weekly	Sunday	12:00 am – 6:00 am
			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.

11.4.2 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.

12.0 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.

12.1 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.

12.2 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.

12.3 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.

12.4 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. The ministry response to the submission can be expected within a week of the form’s submission.

12.4.1 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.

Appendix A: Conformance Test Preparation Checklist

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

1. Pre-Conformance Support Services	
□	Contact Conformance and Integration Services with any questions regarding the Conformance Standards (rules or specifications), network issues or general questions regarding readiness.
2. Conformance Self-test	
□	Run a self-test in the sandbox environment using the provided test plan to confirm the application passes the rules specified in the Conformance Standards. Do this prior to requesting a formal ministry conformance test.
3. Conformance Test Request	
□	Submit a Conformance Initiation Notice to Conformance and Integration Services to schedule a formal conformance test.
4. Environment Readiness	
	For applications using the **HIAL**:
□	Confirm that you have registered, supplied your configuration information and setup a secured connection (certificate signing process) to the conformance environment.
□	Confirm you have the userids to access the conformance environment (these will differ from the ones used in the sandbox environment).
	For applications using **HNSecure**:
□	Confirm you have registered for and received the facility ID to be used for the evaluation. These are different from those used during development.
5. Test Data	
□	Receive and add test data to the POS application prior to the evaluation.
6. Evaluation Location and Facilities	
□	Understand the remote facilities and tools to be used for conducting the evaluation remotely (unless an on-site evaluation is requested). Be available for a pre-test verification of the technology to be used during the conformance testing.
7. Software Organization Presenter Requirements	
	Ensure the application presenter from the software organization:
□	is knowledgeable of the software product and the test cases
□	is able to perform and display all required functions
□	has the ability to provide screen shots upon request
□	has access to technical support if required
□	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
VENDOR APPLICATION FOR CONFORMANCE AND INTEGRATION SERVICES (Form#: HLTH 4637)
CONFORMANCE INITIATION NOTICE (Form#: HLTH 4636)
HNSECURE REGISTRATION - Specific to pharmacy access to PharmaNet
APPLICATION RELEASE ASSESSMENT

Note: To use the forms, save to your local drive, fill-out and send to HLTH.CISSuport@gov.bc.ca