Ministry of Health

# British Columbia
# Professional and Software Conformance Standards

## Electronic Health Information Exchange

## Volume 3A: Business Rules – General

Version 3.3 2021-09-30

Security Classification: Low Sensitivity

**Document Details**

| | |
|---|---|
| Author: | Ministry of Health Conformance and Integration Services |
| Date Created: | 2014-10-09 |
| Last Updated: | 2021-09-30 |
| Version: | 3.3 |

## Table of Contents

# 1.0 Introduction

The rules in this volume define the mandatory standards for all software organizations.

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

- (A) Attest by signing the Vendor Participation Agreement that your product conforms to the stated standard and that documented policy and procedures are maintained for internal purposes or to support an audit;
- (C) Attest to as indicated in (A) and provide a comment. The comment must provide a high-level description of how your product conforms to the stated standard; and
- (D) Attest to as indicated in (A) and demonstrate that your product conforms to the stated standard.

**Note(s):**

- Some of the rules in this volume depend on functionality described in the application enforced rules of Volume 2 (Information Privacy and Security) or Volume 4A (Application Enforced Rules – General).
- Demonstration of the requirements is achieved through completion of an evaluation template and submission of your training materials to the Ministry for evaluation.

## 2.0 General – Business Rules

The following general business rules apply to all points of service (POS) where information is accessed and exchanged with Ministry health information exchange systems.

*Table 1 General – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus1.1 | **Review of Trusted Identity Documentation**<br>Trusted identity documentation must be reviewed to ensure names, birth dates, and gender are correctly entered.<br>Trusted identity documentation includes:<br>• BC Services Card;<br>• Birth Certificate;<br>• Canadian Citizenship ID Card;<br>• Canadian Forces ID Card;<br>• Canadian Record of Landing or Confirmation of Permanent Residence or Permanent Resident Card;<br>• Certificate of Indian Status Card (Aboriginal Affairs and Northern Development Canada – AANDC);<br>• Change of Name Document;<br>• Driver's License;<br>• Marriage Certificate;<br>• Other Provincial Health Insurance Cards (i.e. not BC); and<br>• Passport. | D |
| Bus1.2 | **Alignment with HIE Standards**<br>Users should work with their vendors to identify where their local data may not align with data in a Ministry system (e.g., address format, preferred name storage, phone number format) and remedy the discrepancies. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus1.3 | **Confirm Identity**<br>Before providing treatment, the client's identity must be confirmed using proper documentation:<br>• BC Services Card – with photo:<br>  ○ If the client has a BC Services Card with a photo it must be used to confirm their identity and the PHN used to access their record.<br>• BC Services Card – no photo:<br>  ○ If the client presents a non-photo BC Services Card their identity must be confirmed by viewing a trusted identity document (e.g., a Drivers' Licence) - refer to the Review of Trusted Identity Documents rule above.<br>• No BC Services Card – no PHN:<br>  ○ If the patient does not have their BC Services Card, or claims that they do not have a PHN, use the demographic information they provide and verify their identify using a trusted identity document to locate their record. | D |
| Bus1.4 | **User Support**<br>Users must contact their vendor as primary support to assist with any concern related to using their application, provincial network and Ministry systems.<br>**Note(s):**<br>1. There are a few situations where a Ministry helpdesk should be contacted directly.<br>2. If this is done, the vendor will not be included in any communication regarding that incident.<br>3. These situations are described in the education materials. | D |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus1.5 | **Key Administrative Activities**<br>The connecting organization must have one or more employees specifically assigned to the following activities:<br>• Implementing and operating appropriate privacy and security standards for the connecting organization including (but not limited to):<br>  ○ training staff on privacy and security requirements;<br>  ○ reviewing business processes for compliance with rules as specified by the Ministry;<br>  ○ receiving and responding to privacy- and security-related notifications;<br>  ○ answering privacy and security questions (e.g., from patients);<br>  ○ responding to complaints, incidents, breaches, audits; and<br>  ○ updating policies/procedures.<br>• Establishing and redesigning business processes as required upon the introduction of new functionality for the Ministry HIE service;<br>• Managing staff account access, including:<br>  ○ user enrolment and access management (e.g., new user set up);<br>  ○ changes to user privileges; and<br>  ○ deactivation of old user accounts.<br>• Ensuring that all staff at the connecting organization receive required training; and<br>• Technically supporting the POS application:<br>  ○ receiving and reviewing release notes from their software provider;<br>  ○ receiving and communicating system messages from the software provider (e.g., outages); and<br>  ○ working with the software provider to ensure that a Business Continuity Plan is in place for the connecting organization.<br>**Note(s):** An employee may be dedicated to a single activity or fulfill the functions of more than one activity. | D |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus1.6 | **Health Professional/Support Person Checks Required**<br>Users who will access a HIE service must be appropriately screened through background and reference checks, such as confirmation of identity, education, and professional qualifications, employment data and references. | A |
| Bus1.7 | **Privacy and Security Responsibility**<br>Every member of the connecting organization is ultimately responsible for all applicable privacy and security policies. | C |

## 3.0 Access Management

*Table 2 Access Management – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus2.1 | **Conformant Software**<br>The connecting organization must use conformant software to access Ministry HIE services.<br>**Note(s):** A list of conformant software is available from the Ministry's Conformance and Integration Services. | A |
| Bus2.2 | **Legal Agreement**<br>Every user who accesses a Ministry HIE service must first sign the required legal agreement(s) associated with the HIE service acknowledging all obligations. | A |
| Bus2.3 | **Environments Acceptable Use**<br>The terms specified in the acceptable use policy for non-production environments must be read and abided by. | A |
| Bus2.4 | **HIE Service Availability**<br>If one HIE service (e.g., PharmaNet) is unavailable the user will continue to access the POS application and other available HIE services (e.g., Client Registry, PLIS). | D |
| Bus2.5 | **No Access of HIE Services Outside of Canada**<br>Ministry HIE services must not be accessed from outside of Canada as per provincial legislation. | D |
| Bus2.6 | **Remote Access to the POS Application**<br>Remote access to the POS application must only use the remote access solution that was accepted through the Ministry's conformance evaluation process. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus2.7 | **Technical Support Event Log**<br>A record must be retained for two years or as prescribed in regulation of the support all technical support activities provided by external vendors that have been conducted on computers that access a HIE system or the connecting organization's network, either directly or remotely.<br>The following information must be recorded:<br>• technical support person's name and contact information;<br>• name and contact information of:<br>  ○ the person who authorized the access; and<br>  ○ each person whose name, password, code or other information was used to access the HIE system; and<br>• the date and time of each access.<br>If unsupervised access was provided, the reasons why this was necessary, including all details of any actions taken or attempted must be recorded. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus2.8 | **Access to Ministry HIE Systems**<br>All users requiring access to a HIE service must be authorized.<br>If applying for access, each user's functional role at the connecting organization must be identified appropriately by the access administrator to ensure the correct access is assigned during the registration process.<br>A formal application process must be initiated several days before the user requires access to allow technical configuration changes implemented by the POS software provider and the Ministry.<br>Processes and procedures must be in place to ensure that access to electronic health information (EHI) by personnel and subcontractor personnel is based strictly on role and need to know to maintain patient confidentiality.<br>**Note(s):**<br>1. Access is authorized based on the least privilege necessary for the user's job function (i.e., need to know basis).<br>2. The functional role determines the access permissions available to the user in the POS application and HIE service.<br>3. Each user will be assigned one distinct set of permissions and be prevented access to any service not specifically assigned. | D |
| Bus2.9 | **Access Administrator**<br>Each connecting organization's access administrators are accountable for POS access requirements.<br>This includes:<br>• Adding or removing a user's access (including temporary replacements);<br>• Changing user access permissions (i.e., different job roles);<br>• Ensuring the role does not provide greater access than what is appropriate;<br>• Identifying the most appropriate functional role for each staff member; and<br>• Submitting completed registration forms regarding the above. | D |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus2.10 | **Disable/Remove HIE Access**<br>If a user no longer requires access to HIE services (e.g., change in job function, job termination, end of locum, extended leave, during suspected and actual privacy and security incidents and breaches) the connecting organization must submit a request to the Ministry to have the access disabled (temporarily) or removed (permanently).<br>This function must be assigned to an individual at the connecting organization. | D |
| Bus2.11 | **Reinstate HIE Access**<br>The connecting organization must submit a request to the Ministry to have the access to a disabled HIE account reinstated when required.<br>This function must be assigned to an individual at the connecting organization. | D |

## 4.0 Data Access & Use

*Table 3 Data Access & Use – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus3.1 | **No Browsing**<br>Browsing is not permitted.<br>Users must be providing health services or facilitating care related to the patient prior to searching for the patient in a provincial clinical repository (e.g., PharmaNet, PLIS).<br>In order to search the provincial registries users must be:<br>• providing health services or facilitating care, related to the patient prior to searching for the patient;<br>• identifying an individual who needs or is receiving health services;<br>• identifying a person providing health services; or<br>• facilitating health insurance and health service billing. | D |
| Bus3.2 | **No Modifications of HIE Data**<br>Data received from a Ministry HIE service cannot be modified.<br>However, it may be annotated when stored in the POS application. | D |
| Bus3.3 | **Use or Disclosure of Patient Data**<br>Patient data received from a Ministry HIE service must not be used or disclosed for any purpose other than:<br>• providing care to the individual whose information is being accessed; or<br>• providing a patient with a copy of their own profile. | D |
| Bus3.4 | **Temporary Copies of Patient Data**<br>Temporary copies (e.g., paper forms) of patient data received from a Ministry HIE service must be securely disposed when no longer required for its intended use. | D |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus 3.5 | **Reporting Incidents of Inappropriate Access, Use or Disclosure**<br>Personnel (employees and contractors) must be made aware of procedures for responding to suspected and actual privacy and security incidents and breaches, including "whistle-blower" protection measures. | D |

## 5.0 Clinical Data

The following general business rules apply to points of service that access/exchange clinical health information with Ministry information exchange systems.

Note(s): Masking rules do not apply to Pharmacies.

*Table 4 Clinical Data – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus4.1 | **Confirm Patient Identity**<br>A patient's identity must be confirmed through the Client Registry prior to any other interaction with the patient's EHI.<br>**Note(s):** Connecting organizations not integrated to Client Registry must use the PharmaNet transaction (TID or TPN) for confirming patient identity. | D |
| Bus4.2 | **Reason to Unmask Stored Data**<br>The user must provide a reason prior to unmasking any stored data in the POS application.<br>**Note(s):**<br>1. The user will be alerted when accessing a patient chart containing masked data.<br>2. Reasons for unmasking are logged within the POS application for future audit purposes.<br>3. Stored data in the POS application that has been unmasked will be re-masked when the user has exited the patient chart, or the session has timed-out. | D |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus4.3 | **Display of Current or Previous EHI Data**<br>The user may request display of previous versions of EHI stored in the POS application.<br>**Note(s):**<br>1. The POS application will by default, display the most current version of the business record stored.<br>2. The user will be able to recreate a view of EHI and POS data that comprised the patient record at a point in time. | D |
| Bus4.4 | **Current Data**<br>Ad-hoc requests may be made to check for more recent data from a HIE service repository than what is currently stored in the POS application.<br>For example, users may request updates to all previously stored PLIS data or request another download of a patient's profile from PharmaNet.<br>**Note(s):** If a lab record received from PLIS is opened in the POS application an automatic query is sent to PLIS. | D |
| Bus4.5 | **Data Source**<br>If viewing data in the POS application the user will be able to identify its source (e.g., PNET). | D |

# 6.0 Privacy & Security

This section defines the common business-related information privacy and security rules that must be implemented for accessing the Ministry's Health Information Exchange (HIE) Services.

## 6.1 Patient Records

*Table 5 Patient Records – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus5.1 | **Establish Policies and Procedures**<br>Privacy and security policies and procedures must be established, regularly reviewed and updated as required either at planned intervals and/or when significant changes occur.<br>The content must include the following:<br>• Safeguarding confidentiality of personal health information;<br>• Maintaining patient records:<br>  ○ Printing;<br>  ○ Secure storage;<br>  ○ Retention;<br>  ○ Transport; and<br>  ○ Secure disposal.<br>• Faxing documents containing personal information;<br>• Using couriers to send documents containing personal information;<br>• Reviewing audit logs at scheduled intervals; and<br>• Maintaining user accounts, including deactivating those no longer required. | A |
| Bus5.2 | **Communicate Policies and Procedures**<br>Documented privacy and security policies must be communicated to all staff and external parties (e.g., vendors, suppliers, partners) who have access to the POS application. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus5.3 | **Access Audit Log Review**<br>A designated individual must conduct regular and random internal reviews of the entire system (hardware and networking) and EMR application audit logs to help ensure that users are not accessing EHI, printing or deleting files not directly related to their professional role and provide alerts to the connecting organization's management should suspected anomalies be observed. | A |
| Bus5.4 | **Restricted Audit Log Access**<br>Access to the audit logs and audit tools must be restricted to authorized personnel to prevent misuse or compromise. | A |
| Bus5.5 | **Information Incident Management**<br>Procedures must be established for managing suspected and actual information incidents.<br>If a privacy or security incident involves access to or data received from HIE systems, you must promptly notify the province according to your systems access agreement.<br>**Note(s):**<br>1. An information incident is when unwanted or unexpected events happen that threaten privacy or information security.<br>2. Information incidents are also called privacy breaches when they involve personal information about people (e.g., names, birthdates, social insurance numbers, or client file information).<br>3. A breach can include the loss or theft of personal health information or other unauthorized activities, including unauthorized access that may result in the loss of custody or control over personal health information.<br>4. For more information to ensure your organization is prepared if a breach occurs see Privacy Breaches: Tools and Resources by the Office of the Information Privacy Commissioner for British Columbia (www.oipc.bc.ca/guidance-documents/1428). | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus5.6 | **Patient Privacy Notification**<br>A patient privacy notice or other communication materials that inform patients about information privacy practices must be made readily available. | A |
| Bus5.7 | **Patient Privacy Requests**<br>Procedures for dealing with patient requests for information, corrections, and complaints must be established and openly communicated (e.g., via poster or pamphlet). | A |
| Bus5.8 | **Disposal of Computer Equipment**<br>Before disposing of computer equipment, all personal health information must be permanently removed from the equipment in a manner that ensures the information cannot be reconstructed. | A |
| Bus5.9 | **Contract Privacy Protection Clause**<br>Contracts with third parties that involve EHI (e.g., technology support service) must contain privacy protection obligations, which meet or exceed the contract/agreement privacy and security requirements with the Ministry. | A |
| Bus5.10 | **Confidentiality Agreement**<br>Anyone who may be exposed to EHI (e.g., employees, contractors and third parties) must sign a confidentiality agreement that specifies obligations and expectations including repercussions for inappropriately collecting, using, or disclosing personal information.<br>These agreements must be reviewed and/or renewed annually. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus5.11 | **Annual Privacy and Security Training**<br>All personnel (employees and contractors) must complete Privacy and Security Awareness Training comprised of new employee orientation and regularly scheduled annual refreshers.<br>The content should include:<br>• Privacy and Security polices and related procedures including any changes introduced;<br>• Overview of the connecting organization's security safeguards and staff responsibilities;<br>• Risk mitigation strategies to protect patient information security; and<br>• Steps required for managing a breach in emergency situations. | A |

## 6.2 Account Management

*Table 6 Account Management – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus6.1 | **User ID Requirements**<br>Each user must have:<br>• A unique user ID and password; or<br>• A two factor token when two-factor authentication is used.<br>**Note(s):** Password and tokens must not be shared. | A |
| Bus6.2 | **Password Management**<br>The password for the local computer/terminal used to access a HIE system must meet the following requirements:<br>• Minimum of eight characters;<br>• Changed every 90 days or less (or as required by applicable policy); and<br>• Contain characters from three of the following categories:<br>  ○ uppercase characters<br>  ○ lowercase characters<br>  ○ numerals<br>  ○ non-alphanumeric keyboard symbols | A |
| Bus6.3 | **Transmission of Passwords**<br>Passwords, passphrases and passcodes must be securely communicated and separated from the user ID when transmitted electronically. | A |
| Bus6.4 | **Inactive User Accounts**<br>A user account inactive (or not activated) for 90 days or greater is considered dormant and must be:<br>• Removed from the system; or<br>• Disabled to prohibit login to the system. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus6.5 | **Annual Review of Users**<br>Access reviews of all the connecting organization's users must be performed at a minimum every 90 days to reconcile all active accounts with the list of individuals working at the site.<br>Accounts present for individuals who are no longer with the connecting organization or do not require access must be disabled and removed. | A |

## 6.3 Hardware & Peripherals

*Table 7 Hardware & Peripherals – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus7.1 | **Current Security Patches**<br>Operating system, all plug-in software and application security patches on computers must be kept current using scheduled updates or real-time update protocols (auto-update).<br>Legacy/end-of-support operating systems must not be used. | A |
| Bus7.2 | **Anti-virus Software**<br>Anti-virus software must be installed on all systems (particularly personal computers and servers) and enabled for auto updates, actively running and generating audit logs. | A |
| Bus7.3 | **Personal Desktop Firewalls**<br>Personal desktop firewall (end-point protection) firewalls must be installed and running on computers with high security settings.<br>**Note(s):** Personal firewall software, part of the operating system or purchased commercially separately frequently have default settings configured with a lower security threshold or may be turned off completely. | A |
| Bus7.4 | **Unattended Work Stations**<br>After a defined period of inactivity (maximum of 15 minutes) computers left unattended must automatically lock out all users (e.g., use a screensaver requiring the authorized user to sign on again with a password before restoring screens). | A |
| Bus7.5 | **Monitor Placement**<br>Computer monitors must be situated in a manner that prevents unauthorized viewing. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus7.6 | **Safeguard Mobile Devices**<br>Mobile devices (e.g., laptops, smartphones and iPods) and removable media (e.g., USB drives) containing personal health information must be password protected and encrypted.<br>If these devices are not in the user's direct control, measures must be taken (e.g., by using locking devices with physical locks or equivalent) to protect the device from theft or misuse. | A |
| Bus7.7 | **Peripheral Device Security**<br>Peripheral devices (e.g., printers, fax machines) must be located in secure (non-patient accessible) areas to prevent unauthorized access. | A |

## 6.4 Server & Network

*Table 8 Server & Network – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus8.1 | **Physical Security of Server/Network Equipment**<br>Local server and network equipment must be kept in dedicated, physically secure areas that are only accessible to authorized personnel using physical security measures such as:<br>• Locked and/or bolted (or equivalent) doors and windows;<br>• Locked room(s) with solid wall (floor-to-ceiling) construction or specialized locked cabinet(s) or equivalent;<br>• Monitored alarm systems; and<br>• Restricted key access. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus8.2 | **WLAN Encryption and Security Measures**<br>Wireless local area networks (WLAN) must be encrypted and have security measures that, at a minimum, are equivalent to the Secure Wireless Local Area Network Connectivity Standard as defined by the Ministry:<br>• Physically secure wireless access points<br>• Wi-Fi Protected Access II (WPA2) Enterprise<br>  ○ Authentication: EAP-TLS; and<br>  ○ Encryption: AES-CCMP (128 bits minimum).<br>• Wi-Fi Protected Access II (WPA2) Personal<br>  ○ Authentication Pre-shared keys (PSK) with a minimum 13 characters random passphrase;<br>  ○ PSK must be secured and changed on a regular basis;<br>  ○ PSK must be changed whenever employees/contractors that have access to the network leave the organization; and<br>  ○ Encryption: AES-CCMP (128 bits minimum).<br>**Note(s):**<br>1. Personal mode must only be used for small network installations that do not have authentication servers available.<br>2. Guest Wi-Fi access is completely isolated from the Clinic LAN/Wi-Fi network. | A |
| Bus8.3 | **Managed Perimeter Defence Safeguards**<br>The local area network (LAN) must implement managed perimeter defence safeguards to mediate all traffic and to protect systems from “over the network” attacks and attempts at security breaches. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus8.4 | **Direct Connection to eNG, PPN or SPANBC**<br>There must be no cross connection to an external network (e.g., a commercial internet provider such as Shaw) when your local area network (LAN) is directly connected to the:<br>• eHealth Network Gateway (eNG);<br>• Private Physician Network (PPN); or<br>• Shared Provincial Network (SPANBC). | A |
| Bus8.5 | **Restricted Network Access to Local Server**<br>Firewalls must be installed and running to limit authorized traffic to the local server. | A |
| Bus8.6 | **Files Backup Storage**<br>Backup files must be stored in a secure location, preferably off-site.<br>If backup files are stored off-site, they must be encrypted to a minimum of AES-256. | A |
| Bus8.7 | **Regular System Log Review**<br>The local server must have system logging capabilities enabled and logs must be reviewed regularly.<br>A schedule and procedures must be in place for a designated individual to routinely monitor system logs for unusual patterns or anomalies.<br>Any potential security weaknesses or breaches must be reported to the connecting organization's management. | A |
| Bus8.8 | **Local Server Update Procedures**<br>Procedures and accountability for evaluating and applying operating system, all plug-in software and application updates, hot fixes, and patches must be implemented for the local user.<br>**Note(s):** Updates to server OS and software running on it is typically handled by IT specialist following dedicated procedures in compliance with clinic security policies. | A |

## 7.0 Training & Education

The following rules define the mandatory standards for all software organisations with respect to the development and delivery training and education.

*Table 9 Training & Education – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus9.1 | **User Training**<br>All users must receive training prior to accessing Ministry HIE services.<br>Training must cover software function and features, and related policy, procedures and business rules.<br>**Note(s):**<br>1. All software providers and organizations are required to provide training to their users.<br>2. Subsequent training may be provided by someone at the connecting organization trained for this purpose (e.g., a super user). | A |
| Bus9.2 | **User Education Materials**<br>Users must read the education materials applicable to their job functions prior to accessing Ministry HIE services.<br>Education materials must not be duplicated without permission from the Ministry of Health.<br>**Note(s):** All education materials will be:<br>1. referenced in user training materials; and<br>2. available continuously on the Ministry web site. | A |
| Bus9.3 | **Notification of Updates to User Education Materials**<br>The connecting organization must subscribe to updates on the Conformance and Integration Services website to be notified if there are changes to Ministry-provided education materials. | A |

## 7.1 Training & Education Materials

*Table 10 Training & Education Materials – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus10.1 | **Training Plans and Learning Materials**<br>The following application-specific training plans and learning material addressing the requirements in this volume must be submitted as part of conformance:<br>• A completed evaluation template in response to the domain specific training requirements;<br>• Training Plan document covering key training program elements such as:<br>  ○ Training overview (objectives, audience, points of contact, trainer responsibility, etc.)<br>  ○ Requirements and pre-requisites (mandatory training requirements as per Volume 3A)<br>  ○ Training methods and approach:<br>  1. delivery methods (in-class training, self-service, e-learning)<br>  2. learning material types (manuals, notebooks, online modules, job-aides sheets)<br>  3. training environments (organization, MOH)<br>  4. trainee evaluation (quiz or other methods)<br>• Training curriculum (complete list of training courses that will be developed and delivered) including:<br>  ○ the associated learning objectives<br>  ○ delivery method: in-class, e-Learning, etc.<br>  ○ trainer guide / teaching plan<br>  ○ targeted audience: POS functional roles (prescriber, non-prescriber, clinical support, administrative, system admin) and specific user situations (new functionality, new user, new POS, etc.). | D |
| Bus10.2 | **Integrated Education Materials**<br>Education material must be referenced in the training material along with links directing users to the education web site. | D |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus10.3 | **Training and Education Reference Materials**<br>Users must have access to training and learning materials for ongoing reference. | A |
| Bus10.4 | **Certification Compliance**<br>The POS application must have received a “Interface Approval Notice” prior to user training taking place. | A |
| Bus10.5 | **Material Changes to Training and Education**<br>The Ministry must be contacted in order to determine if significant changes made to system integration-related training materials will require a conformance evaluation. | A |
| Bus10.6 | **Notification of Updates to User Education Materials**<br>Organizations must subscribe to updates on the Ministry’s web site for notification of when there are changes to Ministry-provided education materials. | D |

## 7.2 Training Development & Maintenance

*Table 11 Training Development & Maintenance – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus11.1 | **Documentation Version**<br>All training plans and materials must contain version information, including the date of last review and/or update. | D |
| Bus11.2 | **Spelling and Grammar**<br>Training materials must not contain spelling and/or grammatical errors. | D |
| Bus11.3 | **Current Documentation**<br>All training plans and materials must accurately reflect the application which is being deployed to end-users including:<br>• complete, current workflows with all steps documented; and<br>• screenshots with current window layout, titles, and field names. | D |
| Bus11.4 | **Training Use Case Data**<br>Training use case data must be sufficient to satisfy the training requirements listed in the applicable Volume 3 (Business Rules) for the HIE service (e.g., PharmaNet, PLIS). | A |
| Bus11.5 | **Request Training Data**<br>Software organizations may request the Ministry to provide additional training data to support software-specific training scenarios.<br>**Note(s):** Requests must be made prior to the start of training and in accordance with Ministry protocols. | A |
| Bus11.6 | **Education Material**<br>Ministry-developed education content must not be duplicated without prior approval of the Ministry. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus11.7 | **Impact Assessment**<br>Impact to training and/or materials must be assessed when there are changes in the:<br>• Conformance standards;<br>• Ministry developed education materials; or<br>• Software organization's application.<br>Users must be notified of subsequent changes and provided with the updated related materials.<br>**Note(s):** If the POS application undergoes material changes and requires re-conformance testing, training materials will be evaluated as part of that conformance. | A |
| Bus11.8 | **Notice to Users – Education Material**<br>If notified of changes to education materials those changes must be relayed to end-users. | A |
| Bus11.9 | **Notice to Users – Functionality**<br>POS users must be formally notified of all changes that affect functionality (e.g., system upgrade, application patch) and identify the magnitude of the change.<br>Users must be informed of:<br>• planned changes a minimum of 7 days prior to the change; and<br>• unplanned or emergency change as soon as possible after the change. | A |

## 7.3 Training Delivery

*Table 12 Training Delivery – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus12.1 | **Training Responsibility**<br>All aspects of preparing to deliver application-specific training must be provided including (but not limited to):<br>• scheduling of users and facilities;<br>• arranging for training accounts; and<br>• validating end to end connectivity between the POS and the various training environments.<br>**Note(s):** The Ministry will provide support to training activities within scope of its services (e.g., assigning EHR user IDs for training accounts and support for EHR connectivity). | A |
| Bus12.2 | **Non-Production Environments**<br>All training must take place in non-production environments; and environments must contain fictitious data only.<br>This includes the complete spectrum of systems which will be accessed during training (e.g., POS system and Ministry systems). | A |
| Bus12.3 | **Training Data**<br>Training data and work flows must be an accurate reflection of what users will encounter in the production environment. | A |
| Bus12.4 | **Trainer Access to Training Environments**<br>If a 'Train the Trainer' methodology is being utilized, the connecting organization's trainer must have the appropriate and ongoing access to the training environments, across the end to end spectrum (from the POS application to all Ministry systems).<br>In cases where ongoing access is not continuous, the connecting organization's trainer must be given instructions for how to request and/or enable access to the training environment(s). | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus12.5 | **Functional Training Plans**<br>Training plans and materials must be developed and delivered to end-users specific to their POS functional roles.<br>Functional roles may align with divisions such as the following:<br>• prescribing user (e.g., physician, nurse practitioner, pharmacist)<br>• non-prescribing clinical user (e.g., nurse, medical student)<br>• clinical support user (e.g., clinical MOA, pharmacist technician)<br>• administrative user (e.g., administrative (non-clinical) MOA)<br>• privacy/security/system administration officers | D |
| Bus12.6 | **Training Plans**<br>Training plans and/or approaches for the following specific training situations must be documented:<br>• Existing users/new functionality – training for staff who have already received POS application training, but require training/education for new Ministry exchange service functionality and associated workflows;<br>• New POS - training for staff on the POS application and training/education on the Ministry exchange service functionality and associated workflows;<br>• Existing POS/new staff (including temporary staff) – training for staff new to the already-trained existing POS location; and<br>• Ad hoc – refresher training.<br>**Note(s):** The same training plan may be used for more than one of the above training situations as long as it results in adequate training for the user who finds themselves in the particular training situation. | D |
| Bus12.7 | **'Train the Trainer' Replacement**<br>If a 'Train the Trainer' resource leaves the connecting organization, their replacement must be trained (e.g., repeat the 'Train the Trainer' program) if requested. | A |

| # | Rule | Evaluation Method |
|---|---|---|
| Bus12.8 | **Paper-Based Training Materials**<br>If paper-based training material is provided, users must have access to an adequate supply and/or be provided with a means to print more from a master copy (e.g., soft copy on a CD).<br>All paper-based materials must have a key word index at an appropriate level of detail. | A |
| Bus12.9 | **Self-Service Training Materials**<br>Electronic self-service training and online help must be indexed and key word-searchable by end-users.<br>Examples of this material must be provided. | D |
| Bus12.10 | **Training and Education Outline**<br>Users must be provided with an accessible outline showing the training and education topics and their locations (e.g., page, ID) appropriate for their specific functional role. | D |

## 7.4 Data Conversion & Workflow

Points of Service will require support to ensure their application and workflows are ready to integrate with Ministry exchange services.

*Table 13 Data Conversion & Workflow – Business Rules*

| # | Rule | Evaluation Method |
|---|---|---|
| Bus13.1 | **Workflow Design**<br>Connecting organizations must ensure efficient workflows are incorporated for integrating with Ministry HIE services. | A |
| Bus13.2 | **Data Conversion**<br>Each POS application must be assessed, prior to having production access, to determine whether the EMR data is in alignment with Ministry data standards.<br>If misalignment is found the software organization will work with the connecting organization to determine how they can address the misalignment to minimize the burden to users once in production.<br>**Recommendations:**<br>If misalignment is found:<br>• Provide scripting or data conversion services, where patterns of non-alignment are identified; and<br>• Ensure the data is converted as much as possible before the POS accesses the production environment for Ministry systems. Some examples include (but are not limited to):<br>○ Replacing preferred names (nicknames or shortened names) in the first name field with the legal first name.<br>○ Ensuring mailing addresses (e.g., post office box) are not included in the street address field.<br>○ Ensuring the 'home address' field is the same field verified against the Client Registry.<br>○ Removing phone number prefixes (i.e., prefixed by "1"). | A |

# 8.0 Appendix A: Canada Post Addressing Standards

The Canada Post Addressing Standards are used to define the addressing rules that must be adhered to when sending an address to Ministry systems.

**Note(s):**

1. Some of the rules refer to 'line 1' or 'line 2' which reflects the usual structure of an address.
2. In most cases address 'line 1' will be used to enter the street address and address 'line 2' will be used for other designations (e.g., rural route or PO Box).
3. For clarity please review these rules along with the examples in the following section.

*Table 14 Addressing – Business Rules*

| # | Rule |
|---|---|
| Add1.1 | Use these Canada Post Addressing standards when capturing a permanent physical or permanent mailing address. |
| Add1.2 | The following fields must be provided:<br>• address line 1;<br>• city; and<br>• province. |
| Add1.3 | Do not use special characters in address fields such as:<br>\# , : ; ( ) |
| Add1.4 | Use – (dash) to connect an apartment number to a street number. |
| Add1.5 | Many rural areas have a civic address and a "rural route" address.<br>Civic addresses must be captured in line 1 and the rural address in line 2. |
| Add1.6 | The city and province must be in separate fields. |

| # | Rule |
|---|---|
| Add1.7 | Use abbreviations for the street type and the province.<br>For example, use:<br>• St not Street;<br>• Ave not Avenue;<br>• Rd not Road; and<br>• BC, AB, SK for the province. |
| Add1.8 | Do not enter neighbourhood/municipality specific information in the address lines (e.g., for a Victoria address, do not add a municipality such as Oak Bay or a neighbourhood such as James Bay). |
| Add1.9 | Use the full name of a street address.<br>Do not use slang or abbreviated name (e.g., use Patricia Bay Hwy not Pat Bay Hwy). |
| Add1.10 | Always enter the postal code in the correct alphanumeric format.<br>**Note(s):** The Postal Code is a six-character uniformly structured, alphanumeric code in the form "ANA NAN" where "A" represents an alphabetic character and "N" represents a numeric character. |
| Add1.11 | Use punctuation only where you know it is a standard part of the address (e.g., St. Andrew's Way). |
| Add1.12 | Country Codes are optional, but if included, they must conform to ISO 3166 – Country Codes. |
| Add1.13 | All international addresses must have the name of the country on the last entry of the address. |
| Add1.14 | Additional address information (e.g., Attention or C/O John Smith) must be put in the first address line. |
| Add1.15 | Information such as: Bsmt, Upper, Lower, Pad#, must be put above the street address.<br>In the rare case where there is also a C/O address, the C/O goes in address line 1, the BSMT or Upper or Lower or Pad# would go in address line 2 and the street address would go in address line 3. |

| # | Rule |
|---|---|
| Add1.16 | If the address is a post office box number, it must be on the line above municipality, province and postal code.<br><br>A post office box must only be associated with a mailing address, not the physical location of where a person resides. |

## 9.0 Address Examples

The following are examples of valid addresses.

*Table 15 Canadian Urban Addresses*

| Examples – Canadian Urban Addresses | |
|---|---|
| 10-2202 Cornwall Ave<br>Vancouver BC | (Do not use #10-2202) |
| 1145 Kingsway<br>Vancouver BC | |
| 439 11TH St E<br>North Vancouver BC | (Do not use: East 11th Street)<br>(Do not use: N. Van) |
| 405 North Rd<br>Coquitlam BC | |
| 10-123 Main St NW<br>Montreal QC | |

*Table 16 Canadian Rural/Postal Addresses*

| Examples – Canadian Rural/Postal Addresses |
|---|
| 2765 7th Concession<br>RR 8 Stn Main<br>Millarville AB |
| 4145 Steward Rd<br>PO Box 4001 Stn Yarrow Main<br>Chilliwack BC |

*Table 17 US Addresses*

| Examples – US Addresses |
|---|
| 4417 Brooks St NE<br>Washington DC US |
| 200 Madison<br>Suite 2300<br>Chicago IL US |

*Table 18 Foreign Addresses*

| Examples – Foreign Addresses |
|---|
| 2-2-29 Raidencho Kounosu<br>Saitama JP |
| Stotsmarken 18 DK-2970<br>Horsholm DK |
| 138 Tiyu Road E Tianhe District<br>Guangzhou CN |