Ministry of Health

British Columbia
Professional and Software Conformance Standards

Electronic Health Information Exchange
Volume 3A: Business Rules - General

Version 2.0 2017-03-31

Security Classification: Low Sensitivity

Author:	Ministry of Health Conformance and Integration Services
Date Created:	2014-10-09
Last Updated:	2017-03-31
Version:	2.0

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: 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 Rules

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

Table 1 General Business Rules

#	Rule	Evaluation Method
Bus1.0	**Review of Trusted Identity Documentation** Trusted identity documentation must be reviewed to ensure names, birth dates, and gender are correctly entered. Trusted identity documentation includes: • BC Services Card • Birth Certificate • Canadian Citizenship ID Card • Canadian Forces ID Card • Canadian Record of Landing or Confirmation of Permanent Residence or Permanent Resident Card • Change of Name Document • Driver's License • Marriage Certificate • Certificate of Indian Status Card (Aboriginal Affairs and Northern Development Canada – AANDC) • Passport • Other Provincial Health Insurance Cards (i.e. not BC) **Education Reference:** EBUS.00 Confirm a patient's Identity	D
Bus1.1	**Alignment with EHR Standards** 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. **Education and Training Reference:** N/A	A
Bus1.3	**Confirm Identity** Before providing treatment the client's identity must be confirmed using proper documentation. See Review of Trusted Identity Documentation rule. • BC health card – with photo If the client has a BC health card with a photo it must be used to confirm their identity and the PHN used to access their record. • BC health card – no photo If the client presents a non-photo BC health 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.	D

#	Rule	Evaluation Method
	• No health card, no PHN If the patient does not have their BC health 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. **Education Reference:** EBUS.00 Confirm a patient's Identity	
Bus1.4	**User Support** Users must contact their vendor as primary support to assist with any concern related to using their application, provincial network and ministry systems. **Note:** There are a few situations where an EHR Helpdesk should be contacted directly. When this is done, the vendor will not be included in any communication regarding that incident. These situations are described in the education materials. **Education Reference:** EBUS.10 User Support	D
Bus1.5	**Key Administrative Activities** The POS, regardless of its size, must have one or more employees specifically assigned to the following activities: a) Implementing and operating appropriate privacy and security standards for the POS, including, but not limited to: ○ training staff on privacy and security requirements; ○ reviewing business processes for compliance with rules as specified by the ministry; ○ receiving and responding to privacy- and security-related notifications; ○ answering privacy and security questions (e.g., from patients); ○ responding to complaints, incidents, breaches, audits; and ○ updating policies/procedures. b) Establishing and redesigning business processes as required upon the introduction of new functionality for the ministry HIE service; c) Managing staff account access, including: ○ user enrolment and access management (e.g., new user set up); ○ changes to user privileges; and ○ deactivation of old user accounts. d) Ensuring that all POS staff receive required training; and e) Technically supporting the POS application: ○ receiving and reviewing release notes from their software provider; ○ receiving and communicating system messages from the software	**D**

#	Rule	Evaluation Method
	provider (e.g., outages); and ○ working with the software provider to ensure that the Business Continuity Plan is in place for the POS. **Note:** An employee may be dedicated to a single activity or fulfill the functions of more than one activity. **Education Reference:** EBUS.01 Key Admin Activities	
Bus1.6	**Health Professional / Support Person Checks Required** Users who will access a HIE service must be appropriately screened for verification of personal data such as confirmation of identity, education, and professional qualifications, employment data and references.	**A**

3.0 Access Rules

3.1 General

Table 2 Access Rules - General

#	Rule	Evaluation Method
Bus2.1	**Conformant Software** The POS must use conformant software to access ministry HIE services. **Note:** A list of conformant software is available from the ministry's Conformance and Integration Services. **Education Reference:** N/A	A
Bus2.2	**Legal Agreement** Every user who accesses a ministry HIE service must first sign a legal agreement acknowledging their obligations. **Education Reference:** EBUS.01 Key Administrative Activities	A
Bus2.3	**Environments Acceptable Use** The terms specified in the Acceptable Use Policy for Non-production Environments must be read and abided by. **Education Reference:** N/A	A
Bus2.4	**HIE Service Availability** When one HIE service (e.g., PharmaNet) is unavailable the user will continue to access their POS application and other available HIE services (e.g., Client Registry and PLIS). **Education Reference:** EBUS.10 User Support	D
Bus2.5	**Disable HIE Services** Ministry HIE services must not be accessed from outside of Canada. Access to these services must be disabled if accessing your application from outside of Canada. **Note:** This provides adherence to FOIPPA, PSA and the practitioner agreement. **Education Reference:** N/A	D
Bus2.6	**Remote Access to the Application** Remote access to the application must have in place the following controls: a) Secure remote access technologies such VPN, firewall rules, authentication, encryption (minimum AES-128 bit); b) Audit and monitoring processes during the remote access sessions; c) Automatic disconnect of sessions after a specific period of inactivity; d) Unique identifiable user IDs; e) Multi-factor authentication; f) Devices that meet minimum security configuration (e.g., up-to-date	A

#	Rule	Evaluation Method
	malware protection, latest systems and software patches installed, personal firewall); and **g)** Accessed from a location within Canada, unless otherwise permitted in writing by the ministry in accordance with applicable laws.	
Bus2.7	**Technical Support Event Log** Each technical support event for a HIE system must be approved on a case by case basis by authorized staff for the point of service. A record must be created and retained for a minimum of four years with the following information: a) The technical support person's name and contact information; b) The name and contact information of: i) the person who authorized the access; and ii) each person whose name, password, code or other information was used to access the HIE system; c) the date and time of each access; If unsupervised access was provided, the reasons why this was necessary, including details of the attempts made to take an action.	A

3.2 HIAL Users

Table 3 Access Rules – HIAL users

#	Rule	Evaluation Method
Bus3.1	**Requesting HIE Access** All users (practitioners and support staff) requiring access to a HIE service must be authorized. When applying for access, each user's functional role at the point of service must be identified appropriately by the supervising practitioner to ensure the correct access is assigned during the registration process. 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. **Notes:** 1. Access is authorized based on the least privilege necessary for the user's job function. 2. The functional role chosen determines the access permissions available to the user in the POS and HIE service. **3.** Each user will be assigned one distinct set of permissions and be prevented access to any service not specifically assigned**.**	D

#	Rule	Evaluation Method
	Education Reference: N/A	
Bus3.2	**Requesting HIE Access be Disabled/Removed** When 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 point of service must submit a request to the Ministry to have the access disabled (temporarily) or removed (permanently). This function must be assigned to an individual at the POS. See Key Administrative Activities rule. **Education Reference:** EBUS.01 General	D
Gen3.1	**Reinstate HIE Access** The point of service must submit a request to the ministry to have the access to a disabled HIE account reinstated when required. This function must be assigned to an individual at the POS. See Key Administrative Activities rule.	D

4.0 Data Access/Use

Table 4 Data Business Rules

#	Rule	Evaluation Method
Bus4.1	**No Browsing** *Browsing* is not permitted. 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, Provincial Laboratory Information Solution). To search the provincial registries: • users must be providing health services or facilitating care, related to the patient prior to searching for the patient; or • must have one of the following business needs: ○ to identify an individual who needs or is receiving health services; ○ to identify a person providing health services; ○ to facilitate health insurance and health service billing. **Education Reference:** EBUS.09 Accessing and using Provincial Data	D
Bus4.2	**No Modifications of Data** Data received from a ministry HIE service cannot be modified but may be annotated when stored in the POS application. **Education Reference:** TBUS.06 Use and Disclosure of Patient Data	D
Bus4.3	**Use or Disclosure of Patient Data** Patient data received from a ministry HIE service must not be used or disclosed for any purpose other than: • to provide care to the individual whose information is being accessed; or • to provide to a patient requesting a copy of their own profile. **Education Reference:** EBUS.09 Accessing and Using Provincial Data	D
Bus4.4	**Transient Data** Transient data used for print or display purposes must be disposed of appropriately when no longer required for its intended use. Notes: 1) Data received from a HIE service must be stored in the patient chart. 2) Transient data that is created for display is discarded at the end of a session. 3) System transaction logs are not considered *transitory*.	D

#	Rule	Evaluation Method
	Education Reference: EBUS.09 Accessing and Using Provincial Data	
Bus4.5	**Personnel Restricted Data Access** Processes and procedures must be in place to ensure that access to electronic health information by personnel and subcontractor personnel is based strictly on role and need to know to maintain patient confidentiality.	D
Bus4.6	**Reporting Incidents of Inappropriate Access, Use or Disclosure** 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 Business Rules

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

Note: Masking rules do not apply to Pharmacies

Table 5 Clinical Data Business Rules

#	Rule	Evaluation Method
Gen2.1	**Confirm Patient Identity** A patient's identity must be confirmed through the *Client Registry* prior to any other interaction with the patient's electronic health information. **Note:** Community Pharmacies not integrated to Client Registry must use the pharmacy transaction (TID) for confirming patient identity. **Education Reference:** EGEN.03 EHR Data; ECR.02 Confirm a Patients Identity	D
Gen2.2	**Data Storage** Data received from an HIE service must only be used for delivering clinical care to a patient. **Education Reference:** EGEN.03 EHR Data	D
Gen2.4	**Support** Users must work with their software provider to enable access to ministry HIE services. **Notes:** 1. An EMR provider will be responsible for updating (adding, changing and removing) user access to the POS application. 2. An EMR provider will assist the user through the registration process. **Education Reference:** EGEN.01 EHR User Access	D
Gen2.5	**Supervising Provider** Each supervising provider is accountable for POS access requirements for themselves and all their supervised staff. This includes: a) Identifying the most appropriate functional role for each staff member; b) Ensuring the role does not provide greater access than what is appropriate; c) Adding or removing a user's access (including temporary replacements); d) Changing a user's access permissions (i.e., a user has changed job	D

#	Rule	Evaluation Method
	roles); and e) Submitting completed registration forms regarding the above. **Education Reference:** EGEN.01 EHR User Access	
Gen2.11	**Masking Data Stored in the POS Application** Upon a patient's request all, or a portion, of a patient's stored data must be masked. **Notes:** 1. Masked data will not be masked to the user who initiated the mask. 2. Data will be unmasked only for the user who has provided a reason. **Education Reference:** EGEN.03 EHR Data	D
Gen2.12	**Reason to Unmask Stored data** The user must provide a reason prior to unmasking any stored data on the POS. **Notes:** 1. The user will be alerted when accessing a patient chart containing masked data. 2. Reasons for unmasking are logged within your POS application for future audit purposes. 3. POS data that has been unmasked will be re-masked when the user has exited the patient chart or the session has timed-out. **Education Reference:** EGEN.03 EHR Data	D
Gen2.14	**Display of Current or Previous EHI Data** The user may request display of previous versions of electronic health information stored in their POS application. **Notes:** 1. The POS application will by default, display the most current version of the business record stored. 2. The user will be able to recreate a view of electronic health information and POS data that comprised the patient record at a point in time. **Education Reference:** EGEN.03 EHR Data	D
Gen2.16	**Current Data** Adhoc requests may be made to check for more recent data from an HIE service repository than what is currently stored in the POS application. e.g., users may request updates to all previously stored PLIS data or request	D

#	Rule	Evaluation Method
	another download of a patient's profile from PharmaNet. **Notes:** 1. A *PharmaNet Patient Profile* Request will automatically trigger prior to a prescription being recorded on the POS application. 2. When a lab record received from PLIS is opened in the POS application an automatic query is sent to PLIS. **Education Reference:** EGEN.03 EHR Data	
Gen2.17	**Data Source** When viewing data in the POS application the user will be able to identify its source (e.g., EHR or POS). **Education Reference:** EGEN.03 EHR Data	D

6.0 Privacy and 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 6 Privacy and Security - Patient Records

#	Rule	Evaluation Method
Bus6.1	**Establish Policies and Procedures** Privacy and security policies and procedures must be established and include the following: a) Confidentiality of personal health information; b) Maintaining patient records: • Printing; • Secure storage; • Retention; • Transport; and • Secure disposal. c) Faxing documents containing personal information; d) Using couriers to send documents containing personal information; e) Reviewing audit logs at scheduled intervals; and f) Maintaining user accounts, including deactivating those no longer required. **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.2	**Policies and Procedures Maintenance** The policies and procedures must be regularly reviewed and updated as required, either at planned intervals and/or when significant changes occur. **Education Reference:** EBUS.04 P&S-Patient Records	A

#	Rule	Evaluation Method
Bus6.3	**User Access Audit** A schedule and procedures must be in place for a designated individual to routinely and periodically (i.e., spot audit) monitor user access audit trails (including user access audit reports and user access to masked data and protected HIE information audit reports provided by the POS system) for unusual patterns or anomalies. Any potential security weaknesses or breaches must be reported to and signed off by the POS management. **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.4	**Restricted Audit Log Access** Access to the audit logs and audit tools must be restricted to authorized personnel to prevent misuse or compromise. **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.5	**Information Incident Management** Procedures must be established for managing suspected and actual information incidents to meet, at minimum, the requirements recommended by the Office of Information and Privacy Commissioner for British Columbia. When a privacy or security incident involves access to or data received from ministry systems, you must promptly notify the province according to your systems access agreement. **Notes:** 1. An information incident is when unwanted or unexpected events happen that threaten privacy or information security. Information incidents are also called privacy breaches when they involve personal information about people, such as names, birthdates, social insurance numbers, or client file information. 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. 2. Privacy Breaches: Tools and Resources by the Office of the Information Privacy Commissioner for British Columbia - www.oipc.bc.ca/guidance-documents/1428 **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.6	**Patient Privacy Notification** A patient privacy notice or other communication materials that inform patients about information privacy practices must be made readily available. **Education Reference:** EBUS.04 P&S-Patient Records	A

#	Rule	Evaluation Method
Bus6.7	**Patient Privacy Requests** Procedures for dealing with patient requests for information, corrections, and complaints must be established and openly communicated (e.g., via poster or pamphlet). **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.8	**Disposal of Computer Equipment** 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. **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.9	**Contract Privacy Protection Clause** Contracts with third parties that involve personal information (e.g., technology support service) must contain privacy protection obligations. **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.10	**Confidentiality Agreement** Anyone who may be privy to confidential clinical or patient information (e.g., employees, contractors and third parties) must sign a confidentiality agreement that: a) Specifies obligations and expectations including repercussions for inappropriately collecting, using, or disclosing personal information; and b) Are reviewed/renewed annually with the organization. **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.11	**Annual Privacy and Security Training** All personnel (employees and contractors) must receive annual privacy and security training. The training must include: a) How to maintain privacy and confidentially of personal health information including EHI; and b) How users safeguard their user IDs and passwords, keys, tokens and other access credentials. **Education Reference:** EBUS.04 P&S-Patient Records	A
Bus6.12	**Electronic Health Information Confidentiality** All personnel (employees and contractors) must be informed that data received from the ministry is part of the patient's record and it is the duty of the organization to protect its confidentiality. **Education Reference:** EBUS.04 P&S-Patient Records	A

6.2 Account Management

Table 7 Privacy and Security - Account Management

#	Rule	Evaluation Method
Bus7.1	**User ID Requirements** Each user must have: a) A unique user ID and password; or b) A two factor token when two-factor authentication is used. **Note:** Password and tokens must not be shared. **Education Reference:** EBUS.05 P&S Account Management	A
Bus7.2	**Appropriate Access Level** The level of access provided for each user must match the user's need to know and provide the least privilege necessary based on the user's job function. **Education Reference:** EBUS.05 P&S Account Management	A
Bus7.3	**Transmission of Passwords** Passwords, passphrases and passcodes must be securely communicated and separated from the user ID when transmitted electronically. **Education Reference:** EBUS.05 P&S Account Management	A
Bus7.4	**Inactive User Accounts** A user account inactive (or not activated) for 90 days or greater is considered dormant and must be: a) Removed from the system; or b) Disabled to prohibit login to the system. **Education Reference:** EBUS.05 P&S Account Management	A
Bus7.5	**Annual Review of Users** An annual review must be conducted to confirm each user's role and permissions to access the HIE service.	A

6.3 Hardware and Peripherals

Table 8 Privacy and Security - Hardware and Peripherals

#	Rule	Evaluation Method
Bus8.1	**Current Security Patches** Operating system and application security patches on computers must be kept current using scheduled updates or real-time update protocols. **Education Reference:** EBUS.07 P&S Network	A
Bus8.2	**Anti-virus software** Anti-virus software must be deployed on all systems (particularly personal computers and servers). **Education Reference:** EBUS.07 P&S Network	A
Bus8.3	**Current Anti-virus Mechanisms** Anti-virus mechanisms must be current, actively running, and generating audit logs. **Education Reference:** EBUS.07 P&S Network	A
Bus8.4	**Firewalls** Personal (end-point protection) firewalls must be installed and running on computers. **Education Reference:** EBUS.07 P&S Network	A
Bus8.5	**Unattended Work Stations** 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). **Education Reference:** EBUS.06 P&S Hardware and Peripherals	A
Bus8.6	**Monitor Placement** Computer monitors must be situated in a manner that prevents unauthorized viewing. **Education Reference:** EBUS.06 P&S Hardware and Peripherals	A

#	Rule	Evaluation Method
Bus8.7	**Safeguard Mobile Devices** 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. When 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. **Education Reference:** EBUS.06 P&S Hardware and Peripherals	A
Bus8.8	**Peripheral Device Security** Peripheral devices (e.g., printers, fax machines) must be located in secure (non-patient accessible) areas to prevent unauthorized access. **Education Reference:** EBUS.06 P&S Hardware and Peripherals	A

6.4 Network

Table 9 Privacy and Security - Network

#	Rule	Evaluation Method
Bus9.1	**Security of Information Technology Equipment** Areas that house information technology equipment (e.g., server rooms, network or telecommunications closets) must be protected against unauthorized access by using physical security measures such as: a) Locked room with solid wall (floor-to-ceiling) construction or specialized locked cabinet or equivalent; a) Restricted key access to (a); b) Locks, bolts (or equivalent) on vulnerable doors and windows; and c) Motion detectors and intrusion alarm systems. **Education Reference:** EBUS.07 P&S Network	A

#	Rule	Evaluation Method
Bus9.2	**WLAN Encryption And Security Measures** 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: a) Physically secure wireless access points; b) Wi-Fi Protected Access II (WPA2) Enterprise; • Authentication: EAP-TLS; • Encryption: AES-CCMP (128 bits minimum); c) Wi-Fi Protected Access II (WPA2) Personal; • Authentication Pre-shared keys (PSK) with a minimum 13 characters random passphrase; • PSK must be secured and changed on a regular basis; • PSK must be changed whenever employees/contractors that have access to the network leave the organization; and • Encryption: AES-CCMP (128 bits minimum). **Note:** Personal mode must only be used for small network installations that do not have authentication servers available. **Education Reference:** EBUS.07 P&S Network	A
Bus9.3	**Managed Perimeter Defence Safeguards** 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 **Education Reference:** EBUS.07 P&S Network	A
Bus9.4	**Direct Connection to SPANBC, PPN or eNG** There must be no cross connection to an external network (e.g., a commercial internet provider like Shaw) when your local area network (LAN) is directly connected to the Shared Provincial Network (SPANBC), Private Physician Network (PPN) or eHealth Network Gateway (eNG). **Education Reference:** EBUS.07 P&S Network	A

6.5 Local Server

The rules in the next table apply to a POS that stores ministry EHI on a local server.

Note: Applications such as medical practice EMRs are housed in application and data hosting centres; therefore the rules in this table do not apply to those locations.

Table 10 Privacy and Security - Local Server

#	Rule	Evaluation Method
Bus10.1	**Secure Area for Local Server** The local server must be housed in a physically secure area as described in Bus9.1 with proper environmental conditions (temperature, humidity and power sources) **Education Reference:** EBUS.08 P&S Local Server	A
Bus10.2	**No Unauthorized Access** Unauthorized personnel must not be permitted into the server area. **Education Reference:** EBUS.08 P&S Local Server	A
Bus10.3	**Restricted Network Access** The following must be implemented in the server environment: a) Operating system and application security patches must be kept current using scheduled updates or real-time update protocols; b) Anti-virus software must be deployed, current, actively running, and generating audit logs; c) Firewalls must be installed and running; and d) Managed perimeter defence safeguards must be used to mediate all traffic and to protect systems from "over the network" attacks and attempts at security breaches. **Education Reference:** EBUS.08 P&S Local Server	A
Bus10.4	**Business Continuity and Disaster Recovery** All local servers with operationally critical data must have documented back-up, system and application restoration (including configurations), and data restoration procedures to support business continuity and disaster recovery planning. **Education Reference:** EBUS.08 P&S Local Server	A

#	Rule	Evaluation Method
Bus10.5	**Files Backup Storage** Backup files must be stored in a secure location, preferably off-site. If backup files are stored off-site, they must be encrypted to a minimum of AES-256. **Education Reference:** EBUS.08 P&S Local Server	A
Bus10.6	**Regular System Log Review** The local server must have system logging capabilities enabled and logs must be reviewed regularly. A schedule and procedures must be in place for a designated individual to routinely monitor system logs for unusual patterns or anomalies. Any potential security weaknesses or breaches must be reported to the POS management. **Education Reference:** EBUS.08 P&S Local Server	A
Bus10.7	**Update Procedures** Procedures and accountability for evaluating and applying operating system and application updates, hot fixes, and patches must be implemented. **Education Reference:** EBUS.08 P&S Local Server	A
Bus 10.8	**Environmental Controls** Environmental controls must be provisioned and properly maintained, including but not limited to: a) uninterrupted power supply to facilitate an orderly shutdown process; b) fire detection and suppression; c) temperature and humidity controls; and d) water damage detection and mitigation. **Education Reference:** EBUS.08 P&S Local Server	A

7.0 Training Development and Delivery

7.1 Training and Education

Table 11 Training and Education Rules

#	Rule	Evaluation Method
Bus5.1	**User Training** All users must receive training prior to accessing ministry HIE services. Training must cover software function and features, and related policy, procedures and business rules. **Notes:** 1. All software providers and organizations are required to provide training to their users. Subsequent training may be provided by someone at the POS trained for this purpose (e.g., a super user). **Education Reference:** EBUS.02 Training	A
Bus5.2	**User Education Materials** Users must read the education materials applicable to their job functions prior to accessing ministry HIE services. Education materials must not be duplicated without permission from the Ministry of Health. **Notes:** 1. All education materials will be referenced in user training materials. 2. All education materials will be available continuously on the ministry web site. **Education Reference:** EBUS.03 Education	A
Bus5.3	**Notification of Updates to User Education Materials** To be notified when there are changes to ministry-provided education materials, the POS must subscribe to updates on the Conformance and Integration Services website. **Education Reference:** EBUS.03 Education	A

7.2 Training and Education Materials

Table 12 Training and Education Rules

#	Rule	Evaluation Method
CM1.1	**Training Plans and Learning Materials** The following application-specific training plans and learning material addressing the requirements in this volume must be submitted as part of conformance: a) A completed evaluation template (template provided) in response to the domain specific training requirements; b) Training plans covering all required functionality for each functional role; c) A full set of the final training materials (e.g., scripts, workbooks, self-service materials) that will be used by end users); d) Description of training methodologies used (e.g., paper, face to face, video, train the trainer); e) A user accessible outline of appropriate training topics for each functional role; f) Training documentation for various training situations as defined in CM3.9; and g) Trainer guide / teaching plan (if required for CM3.15).	D
CM1.2	**Integrated Education Materials** Education material must be referenced in the training material along with links directing users to the education web site.	D
CM1.3	**Training and Education Reference Materials** Users must have access to training and learning materials for ongoing reference.	A
CM1.4	**Certification Compliance** The POS application must have received a “Letter of Compliance” prior to user training taking place.	A
CM1.5	**Material Changes to Training and Education** 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
CM1.6	**Notification of Updates to User Education Materials**	D

#	Rule	Evaluation Method
	Organizations must subscribe to updates on the ministry's web site for notification of when there are changes to ministry-provided education materials.	

7.3 Development and Maintenance

Table 13 Rules for Development and Maintenance of Training and Education Materials

#	Rule	Evaluation Method
CM2.1	**Documentation Version** All training plans and materials must contain version information, including the date of last review and/or update.	D
CM2.2	Training materials must not contain spelling and/or grammatical errors.	D
CM2.3	**Current Documentation** All training plans and materials must accurately reflect the application which is being deployed to end users, including: a) complete, current workflows with all steps documented; and b) screenshots with current window layout, titles, field names, etc.	D
CM2.4	**Training Use Case Data** Training use case data must be sufficient to satisfy the training requirements listed in Volume 3x.	A
CM2.5	**Request training data** Software Organizations may request the ministry to provide additional training data to support software-specific training scenarios. **Note**: Requests must be made prior to the start of training and in accordance with ministry protocols.	A
CM2.6	**Education Material** Ministry-developed education content must not be duplicated without prior approval of the ministry.	A
CM2.7	**Impact Assessment** Impact to training and/or materials must be assessed when there are changes in the: • Conformance Standards	A

#	Rule	Evaluation Method
	• Ministry developed education materials • Software organization's application. POS users must be notified of subsequent changes and provided with the updated related materials. **Note:** If the POS application undergoes material changes and requires re-conformance testing, training materials will be evaluated as part of that conformance.	
CM2.8	**Notice to Users – Education Material** When notified of changes to education materials those changes must be relayed to end users.	A
CM2.9	**Notice to Users – Functionality** 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. Users must be informed of: • A planned changes a minimum of 7 days prior to the change; and • An unplanned or emergency change as soon as possible after the change takes place.	A

7.4 Training Delivery

Table 14 Rules for the Delivery of Training and Education

#	Rule	Evaluation Method
CM3.1	**Training Responsibility** All aspects of preparing to deliver application-specific training must be provided including, but not limited to: • scheduling of users and facilities; • arranging for training accounts; and • validating end to end connectivity between the POS and the various training environments. **Note**: 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

#	Rule	Evaluation Method
CM3.4	**Non-production Environments** All training must take place in non-production environments. Environments must contain fictitious data only. This includes the complete spectrum of systems which will be accessed during training (e.g., POS system and ministry systems).	A
CM3.5	**Training Data** Training data and work flows must be an accurate reflection of what users will encounter in the production environment.	A
CM3.6	**Trainer Access to Training Environments** If a 'Train the Trainer' methodology is being utilized, the POS-based 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). In cases where ongoing access is not continuous, the POS-based trainer must be given instructions for how to request and/or enable access to the training environment(s).	A
CM3.8	**Functional Training Plans** Training plans and materials must be developed and delivered to end users specific to their POS functional roles. Functional roles may align with divisions such as the following: • Prescribing user (e.g., Physician, Nurse Practitioner, Pharmacist) • Non-Prescribing clinical user (e.g., Nurse, Medical Student) • Clinical support user (e.g., Clinical MOA, Pharmacist technician) • Administrative user (e.g., Administrative (non-clinical) MOA) • Privacy / security / system administration officers	D
CM3.9	**Training Plans** Training plans and/or approaches for the following specific training situations must be documented: • 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; • New POS - training for staff on the POS application and training/education on the Ministry exchange service functionality and associated workflows; • Existing POS/new staff (including temporary staff) – training for staff	D

#	Rule	Evaluation Method
	new to the already-trained existing POS location; and • Ad Hoc – refresher training. **Note**: 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.	
CM3.10	**'Train the Trainer' Replacement** If a 'Train the Trainer' resource leaves the POS, their replacement must be trained (e.g., repeat the 'Train the Trainer' program) if requested by their client.	A
CM3.11	**Paper-based Training Materials** 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). All paper based materials must have a key word index at an appropriate level of detail.	A
CM3.12	**Self-service Training Materials** Electronic self-service training and online help must be indexed and key-word-searchable by end users. Examples of this material must be provided.	D
CM3.13	**Training and Education Outline** 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

7.5 Data Conversion and Workflow

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

Table 15 Data Conversion and Workflow Support Rules

#	Rule	Evaluation Method
CM4.1	**Workflow Design** Organizations must work with each POS to ensure efficient workflows are incorporated for integrating with ministry HEI services.	A

#	Rule	Evaluation Method
CM4.2	**Data Conversion** Each POS must be assessed, prior to having production access, to determine whether the EMR data is in alignment with Ministry data standards. If misalignment is found the software organization will work with the POS to determine how they can address the misalignment to minimize the burden to users once in production. **Recommendations:** If misalignment is found: • Provide scripting or data conversion services, where patterns of non-alignment are identified; and • 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: ○ Replacing preferred names (nicknames or shortened names) in the first name field with the legal first name. ○ Ensuring mailing addresses (e.g., post office box) are not included in the street address field. ○ Ensuring the 'home address' field is the same field verified against the Client Registry. ○ Removing phone number prefixes (i.e., prefixed by "1").	A