Ministry of Health

British Columbia

Professional and Software Conformance Standards

Electronic Health Information Exchange

Volume 3: Business Rules
General – All Points of Service

Version 0.2 2014-11-24

Security Classification: Low Sensitivity

Author:	Ministry of Health Conformance and Integration Services
Date Created:	2014-10-09
Last Updated:	2014-11-24
Version:	0.2

Table of Contents

Tables

1.0 Introduction

Organizations developing interfaces to health information exchange (HIE) systems 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 systems.

1.1 Conformance Standards Volume Set

The Conformance Standards are the central reference for organizations wanting to integrate their *Points of Service (POS)* applications with Ministry HIE *systems*. 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 technial message and transport specifications. The Conformance Standards are available on the Conformance and Integration Services website: http://www.health.gov.bc.ca/access/software_development.html.

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 business rules for the users at a *point of service (POS)* who are access/exchange ministry electronic health information with Ministry information exchange systems.

1.4 Intended Audience

The intended audience for this document is:

- **Information Consumers** – who access electronic health information from a Ministry or provincial *data repository* (e.g., end users);
- **Information Custodians** – who maintain or administer *electronic health information* (EHI) resources on behalf of the Information Authority;
- **Information Authority** – who have the responsibility and decision making authority for EHI throughout its lifecycle, including creating, classifying, restricting, regulating, and administering its use or disclosure;
- **Data Providers** – who provide data to, or exchange data with a Ministry data repository (e.g., system to system upload);
- **Software Organizations** – organizations (including in-house system development teams) who develop interfaces to health information exchange systems 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

For mor information or questions regarding the Conformance Standards should be directed to Conformance and Integration Services at: HLTH.CISSupport@gov.bc.ca

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	Education and Training Reference
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)	ECR.02 Confirm Client Identity TCR.02 Confirm Client Identity
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. Notes: 1. If this is not done prior to using the ministry systems, the Point of Service may experience a difficult transition.	TGEN.02 Alignment with EHR Standards
Bus1.2	**Training Environments Acceptable Use** The terms specified in the Acceptable Use Policy for Non-production Environments must be read and abided by.	EGEN.01 EHR User Access
Bus1.3	**Confirm Patient Identity** Before providing treatment the client's identity must be confirmed using proper documentation. • 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 find the client in the PharmaNet.	EGEN.01 EHR User Access ECR.02 Confirm a Patient's Identity TCR.02 Confirm Client Identity TCR.03 Confirm a

#	Rule	Education and Training Reference
	• <u>BC health card – no photo</u> 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. • <u>No health card, no PHN</u> 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 them in PharmaNet.	Patient's Identity: BC Health Card with Photo Presented (Match) TCR.04 Confirm a Patient's Identity: BC Health Card with Photo Presented (Mismatch) TCR.05 Confirm a Patient's Identity: BC Health Card without Photo Presented (Match) TCR.06 Confirm a Patient's Identity: No BC Health Card or PHN Presented (Match
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. Notes: 1. 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.	EGEN.02 User Support TGEN.03 User Support

2.1 Access Rules – General

Table 2 Access Rules - General

#	Rule	Education and Training Reference
Bus2.1	**Conformant Software** The Point of Service must use conformant software to access ministry systems. Notes: 1. A list of conformant software is available from the ministry's Conformance and Integration Services.	NA
Bus2.2	**Legal Agreement** Every user who accesses a ministry system must first sign a legal agreement acknowledging their obligations.	Not yet written

#	Rule	Education and Training Reference
Bus2.2	**Key Administrative roles** Resources conducting key POS administrative roles must be identified and appropriate training directed to each as part of the readiness assessment process. These roles must be defined for each POS, regardless of size. Notes: 1. An employee may be dedicated to a single role or fulfill the functions of more than one role. 2. The point of service, regardless of its size, must have one or more employees specifically assigned to the following activities: • 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. • establishing and redesigning business processes as required upon the introduction of new functionality for the Ministry interface. • managing staff account access. • ensuring that all staff receive required training. • technically supporting the POS application: ○ receiving and reviewing release notes from the software provider, and ○ receiving and communicating system messages from the software provider (e.g., outages). ○ working with the software provider to ensure that the Business Continuity Plan is in place for the POS. • An employee may be dedicated to a single activity or fulfill the functions of more than one activity.	Not yet written

2.2 Access Rules – HIAL Users

Table 3 Access Rules – HIAL users

#	Rule	Education and Training Reference
Bus3.1	**Authorized Access** All users (both health professionals and support staff) requiring	EGEN.01 EHR User Access

#	Rule	Education and Training Reference
	access to ministry systems must be authorized. Notes: 1. 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.	
Bus3.3	**Requesting Access be Removed** When a user no longer requires access to ministry systems (e.g., change in job function, job termination, end of locum, extended leave) the organization must submit a request to the Ministry to have the access deactiviated. Notes: 1. This function must be assigned to an individual at the POS. See Key Administrative Activities rule.	Not yet written

2.3 Clinical Data

Table 4 Clinical Data Business Rules

#	Rule	Education and Training Reference
Bus4.1	**No General Browsing** There must be a business or clinical prerequisite to search for clients and client data. General browsing is not permitted and may be harshly penalized.	EGEN.01 EHR User Access ECR.03 Find Patient
Bus4.2	**Annotations** 1. EHI data cannot be modified but may be annotated when stored in the POS application.	EGEN.03 EHR Data TGEN.06 Annotations

2.4 Training and Education

Table 5 Training and Education Rules

#	Rule	Education and Training Reference
Bus5.1	**User Training** All users must receive training prior to accessing ministry systems. Training must cover software function and features, and related policy, procedures and business rules as indicated in the applicable Change Management and Training volumes. Notes:	EGEN.02 User Support EBus.02 Training TBUS1.02 Training

#	Rule	Education and Training Reference
	1. All software providers 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 superuser). 2. The training requirements are provided in the Conformance Standards, Volume 6 – Change Management and Training.	
Bus5.2	**User Education Materials** Users must read the education materials applicable to their job functions prior to accessing ministry systems. 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.	EBus.03 Education TBUS1.03 Education
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.	EBus.03 Education TBUS1.03 Education
Bus5.4	**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 interface; 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	EBus.01 Key Admin Activities TBUS1.01 Key Admin Activities

#	Rule	Education and Training Reference
	e) Technically supporting the POS application: ○ receiving and reviewing release notes from their software provider; ○ receiving and communicating system messages from the software provider (e.g., outages); and ○ working with the software provider to ensure that the Business Continuity Plan is in place for the POS. Notes: 1. An employee may be dedicated to a single activity or fulfill the functions of more than one activity.	
Bus5.5	**Trainer Replacement** If the POS relies on trainers internal to their organization (e.g., super users trained by the software provider), such trainers must be fully trained in the software's function and features, and related policy, procedures and business rules. Notes: 1. Users may request vendor-provided training for all POS trainers (e.g., super users) and their replacements.	Ebus.02 Training TBUS1.02 Training
Bus5.6	**Training Evaluation** All users who receive training, including those trained by a POS trainer (super user), will receive a training evaluation feedback form from their software provider.	Ebus.02 Training TBUS1.02 Training

3.0 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.

Table 6 Privacy and Security - Patient Records

#	Rule	Education & Training Reference
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 • 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.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
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.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
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 for unusual patterns or anomalies. Any potential security weaknesses or breaches must be reported to the POS management.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
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.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records

#	Rule	Education & Training Reference
Bus6.5	**Privacy and Security Incidents or Breach** Procedures that meet, at a minimum, requirements recommended by the Office of Information Privacy Commissioner for British Columbia must be established for managing suspected and actual privacy and security incidents and breaches. 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. Note: 1. Privacy Breaches: Tools and Resources by the Office of the Information Prevacy Commissioner for British Columbia - www.oipc.bc.ca/guidance-documents/1428	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
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.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
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).	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
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.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
Bus6.9	**Contract Privacy Protection Clause** Contracts with third parties that involve personal information (e.g., technology support service) must contain privacy protection obligations.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
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.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records
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; and b) How users safeguard their user IDs and passwords, keys, tokens and other access credentials.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records

#	Rule	Education & Training Reference
Bus6.12	**Electronic Health Information Confidentiality** All personnel (employees and contractors) must be informed that EHI received from the ministry is part of the patient's record and it is the duty of the organization to protect its confidentiality.	EBus.04 P&S-Patient Records TBUS2.01 P&S – Patient Records

3.1 Account Management

Table 7 Privacy and Security - Account Management

#	Rule	Education & Training Reference
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. Notes: 1. Password and tokens must not be shared.	EBus.05 P&S Account Management TBUS2.02 P&S – Account Management
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.	EBus.05 P&S Account Management TBUS2.02 P&S – Account Management
Bus7.3	**Transmission of Passwords** Passwords, passphrases and passcodes must be securely communicated and separated from the user ID when transmitted electronically.	EBus.05 P&S Account Management TBUS2.02 P&S – Account Management
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.	EBus.05 P&S Account Management TBUS2.02 P&S – Account Management

3.2 Hardware and Peripherals

Table 8 Privacy and Security - Hardware and Peripherals

#	Rule	Education & Training Reference

#	Rule	Education & Training Reference
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.	EBus.07 P&S Network TBUS2.04 P&S Network
Bus8.2	**Anti-virus software** Anti-virus software must be deployed on all systems (particularly personal computers and servers).	EBus.07 P&S Network TBUS2.04 P&S Network
Bus8.3	**Current Anti-virus Mechanisms** Anti-virus mechanisms must be current, actively running, and generating audit logs.	EBus.07 P&S Network TBUS2.04 P&S Network
Bus8.4	**Firewalls** Personal (end-point protection) firewalls must be installed and running on computers.	EBus.07 P&S Network TBUS2.04 P&S Network
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 log on again).	EBus.06 P&S Hardware and Peripherals TBUS2.03 P&S Hardware and Peripherals
Bus8.6	**Monitor Placement** Computer monitors must be situated in a manner that prevents unauthorized viewing.	EBus.06 P&S Hardware and Peripherals TBUS2.03 P&S Hardware and Peripherals
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.	EBus.06 P&S Hardware and Peripherals TBUS2.03 P&S Hardware and Peripherals
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.	EBus.06 P&S Hardware and Peripherals TBUS2.03 P&S Hardware and Peripherals

3.3 Network

Table 9 Privacy and Security - Network

#	Rule	Education & Training Reference
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; b) Restricted key access to (a); c) Locks, bolts (or equivalent) on vulnerable doors and windows; and d) Motion detectors and intrusion alarm systems.	EBus.07 P&S Network TBUS2.04 P&S Network
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). Notes: 1. Personal mode must only be used for small network installations that do not have authentication servers available.	EBus.07 P&S Network TBUS2.04 P&S Network
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.	EBus.07 P&S Network TBUS2.04 P&S Network
Bus.30	**Direct Connection to SPANBC or PPN** 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) or Private Physician Network (PPN).	EBus.07 P&S Network TBUS2.04 P&S Network

3.4 Local Server

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

Note: Medical Practice applications 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	Education & Training Reference
Bus10.1	**Secure Area** The local server must be housed in a physically secure area with proper environmental conditions (temperature, humidity and power sources) and protected against unauthorized access by using the following physical security measures: a) Locked room with solid wall (floor-to-ceiling) construction or specialized locked cabinet or equivalent; b) Restricted key access to (a); c) Locks, bolts (or equivalent) on vulnerable doors and windows; and Motion detectors and intrusion alarm systems.	EBus.08 P&S Local Server TBUS2.05 P&S Local Server
Bus10.2	**No Unauthorized Access** Unauthorized personnel must not be permitted into the server area.	EBus.08 P&S Local Server TBUS2.05 P&S Local Server
Bus10.3	**Restricted Network Access** The following must be implemented in the server environment: • Operating system and application security patches must be kept current using scheduled updates or real-time update protocols. • Anti-virus software must be deployed, current, actively running, and generating audit logs. • Firewalls must be installed and running. • 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.	EBus.08 P&S Local Server TBUS2.05 P&S Local Server
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.	EBus.08 P&S Local Server TBUS2.05 P&S Local Server
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.	EBus.08 P&S Local Server TBUS2.05 P&S Local Server

#	Rule	Education & Training Reference
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.	EBus.08 P&S Local Server TBUS2.05 P&S Local Server
Bus10.7	**Update Procedures** Procedures and accountability for evaluating and applying operating system and application updates, hot fixes, and patches must be implemented for the local server.	EBus.08 P&S Local Server TBUS2.05 P&S Local Server
Bus 10.8	**Environmental Controls** Environmental controls must be provisioned and properly maintained, including but not limited to: 1. uninterrupted power supply to facilitate an orderly shutdown process; 2. fire detection and suppression; 3. temperature and humidity controls; and 4. water damage detection and mitigation.	TBD