BRITISH COLUMBIA | Ministry of Health

British Columbia
Professional and Software Conformance Standards

Electronic Health Information Exchange

Volume 4A: Application Enforced Rules – General

Version 3.4 2022-05-20

Security Classification: Low Sensitivity

Copyright Notice

Disclaimer and Limitation of Liabilities

Document Details

Author:	Ministry of Health Conformance and Integration Services
Date Created:	2011-01-04
Last Updated:	2022-05-20
Version:	3.4

Table of Contents

1.0 Application Enforced Rules (for all Points of Service)

The application enforced rules in this section apply to all point-of-service (POS) applications accessing the Ministry's health information exchange (HIE) services:

- Client Registry
- Provider and Location Registry (PLR)
- PharmaNet
- Provincial Laboratory Information Solution (PLIS)

There are two columns in the following tables:

- "Integration" – for applications that store data from one of the HIE services.
- "Viewer" – for applications that do not store data from one of the HIE services.

1.1 General

Table 1 General – Application Enforced Rules

#	Rule	Integration	Viewer
GenTx1.1	**Identifying Protected HIE Information on Display** If protected data (i.e. a patient's access word is assigned to the PharmaNet or PLIS record) is displayed or stored in the POS application, all screens related to the patient's protected data must indicate the record is protected by a patient's access word.	✓	✓
GenTx1.2	**Disable HIE Services** A user must be able to disable all HIE services and continue to use their POS application. **Note(s):** This rule assists the user in adhering to FOIPPA - personal information must be stored and accessed only in Canada.	✓	

1.2 Data Presentation

Application enforced rules in the following table are applicable to any POS applications accessing a ministry system containing clinical data.

Therefore, these rules do not apply to access/exchange data with the Health Registries (i.e., Client Registry or PLR).

Table 2 Data Presentation – Application Enforced Rules

#	Rule	Integration	Viewer
GenTx2.1	**Storage of Complete Business Record** The POS application must store the business record data (e.g., local dispense or prescription) as displayed to the user and the: • timestamp (if stored); • data source (e.g., HIE); and • any other associated metadata.	✓	
GenTx2.2	**Presentation of Clinical Data** If presenting clinical data to the user, the POS application must: • identify its source (e.g. EHR or POS); and • distinguish the display of EHR data from data sourced from the POS system.	✓	✓
GenTx2.3	**Display of Current Version** For HIE data stored at the POS application, by default, the most current version of the business record must be displayed, with previous versions displayed if requested by the user.	✓	
GenTx2.4	**No Modification of Stored HIE Data** HIE data stored in the POS application must not be modified, but may be annotated when stored in the POS application.	✓	

#	Rule	Integration	Viewer
GenTx2.5	**Date Format** All dates displayed must be well-defined to avoid confusion between the day and the month portion of a date (e.g., expansion of year and month such as DD-MMM-YYYY or MMM-DD-YYYY).	✓	✓
GenTx2.6	**Screen Displays** All active display screens must persistently display the patient's: • name; • PHN; • date of birth; and • gender. **Note(s):** Persistent display means when the user scrolls down the screen, the fields indicated above must always be in view to the user.	✓	✓
GenTx2.7	**HIE Service Availability** An HIE service being unavailable must not interrupt user access to their POS application or other available HIE services. For example, if PharmaNet is not available, users must be able to access their POS application and other HIE services (e.g., Client Registry, PLIS).	✓	✓

#	Rule	Integration	Viewer
GenTx2.8	**Printed Data** Print outs containing patient information must include the following in the header or footer on every page: a) patient's full name; b) PHN; c) date and time the report was printed; d) identity of the user who printed the report (e.g., UserID); e) a confidentiality clause indicating the report contains confidential personal information intended solely for the person(s) providing or supporting direct care to the patient; f) source(s) of the data (e.g., "this information includes data received from the Provincial Laboratory Information Solution", "this information includes data received from PharmaNet"); and g) a visual indication that multi-page printed hardcopy is complete (e.g., "page 1 of 1", "page 3 of 5"). **Note(s):** See Volume 4C: Application Enforced Rules – PharmaNet for PharmaNet specific rules.	✓	✓

1.3 Identity Management

Table 3 Identity Management – Application Enforced Rules

#	Rule	Integration	Viewer
GenTx3.1	**User Access** Once logged into the POS application there must be no additional logon required for the user to access a ministry health information service. **Note(s):** The existence of this user logon identifier will be verified within the ministry system.	✓	✓
GenTx3.2	**User Roles** User functionality must be restricted in accordance with the user's business role (e.g., system admin cannot access HIE system data; only prescribers prescribe drugs; only practitioners and support staff can update Provider and Client Registry, other roles cannot). **Note(s):** See Volume 4C: Application Enforced Rules – PharmaNet, Appendix D: PharmaNet User Role Types for details specific to PharmaNet access.	✓	✓
GenTx3.3	**Display All Error Messages** All error messages returned by the HIE service, related to the verification and authorization of user logon identifier with its service, must be displayed to the user.	✓	✓

1.4 View and Storage of Data

The application enforced rules in the following table are applicable to any POS application used to view or store data retrieved from a ministry system containing clinical data.

These rules do not apply to access/exchange of data with registry systems (i.e., Client Registry or PLR).

Table 4 View and Storage of Data – Application Enforced Rules

#	Rule	Integration	Viewer
GenTx4.1	**Access through Patient Chart** Access to ministry data must only be permitted through the patient's existing patient record in the POS system. If a patient chart does not exist, a new patient chart must be created before the query can be initiated.	✓	✓
GenTx4.2	**Current Data** The POS application must support the user in ad-hoc requests to check if more recent data is available in the EHR to what was previously stored in the POS application and, if more recent data does exist: a) support the user in storing the updated data in the POS system; b) create a new record(s) for new data; c) do not alter previously stored data; and d) record the date/time of the record creation in the POS system.	✓	

#	Rule	Integration	Viewer
GenTx4.3	**Consistent Functionality** The POS application must apply the same functionality to HIE data stored in the patient chart as it does to other data stored in the patient chart. This includes: a) displaying, b) sorting, c) filtering, d) graphing, and e) trending.	✓	
GenTx4.4	**Patient Session** Patient data must not be displayed after the associated patient session ends (i.e., when the patient record closes so must all displays of associated data).	✓	✓

1.5 Masking

The application enforced rules in the following table are applicable to data retrieved using a protective word and stored from a ministry system containing clinical data.

Therefore, these rules do not apply to access/exchange of data with registry systems (i.e., Client Registry or PLR).

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

Table 5 Masking – Application Enforced Rules

#	Rule	Integration	Viewer
GenTx5.1	**Masking Stored Data Retrieved with a Protective Word** For data retrieved using a protective word, authorized users must have the ability to: a) mask data in the POS application at the: i. chart level; and ii. record level (e.g., lab record, prescription, dispense). b) unmask previously masked data. Individually masked data (i.e., record masking) must be explicitly selected to unmask. Record masking must be maintained when a new version of the data is received (e.g., new versions of the record must be automatically masked).	✓	
GenTx5.2	**Masking Alert** The POS application must alert users when accessing a patient chart with masked data, that all or a portion of the patient chart is masked.	✓	

#	Rule	Integration	Viewer
GenTx5.3	**Reason to Unmask** If masked data is selected for unmasking, the user must be prompted to enter a reason to unmask stored data (e.g., providing a drop-down box displaying: Emergency, Patient Consent Obtained, Other - include free text space for documenting). The reason for unmasking must be entered before the POS application unmasks and presents the data.	✓	
GenTx5.4	**No Global Unmasking Permitted** Global unmasking of POS data is not permitted. Data that is temporarily unmasked in the POS application must only be made available to the user who has provided a reason for unmasking.	✓	
GenTx5.5	**Automatic Re-Masking** The POS application must be configured to re-mask the unmasked data upon exiting the patient chart or session time-out.	✓	
GenTx5.6	**Logging Access to Masked Data** The application must create a time stamped audit record each time a user access masked data along with the reason to unmask the data.	✓	
GenTx5.7	**Access to Masked Data Audit Reports** The application must be capable of generating user defined reports to provide, at a minimum: a) Reports by patient: Identifying all users who have accessed, or modified a given patient's masked record(s) over a given time; and b) Reports by user: Identifying all masked records accessed by a given user over a given period.	✓	

#	Rule	Integration	Viewer
GenTx5.8	**POS Masked Data** Masked data must not be masked to the user who initiated the mask.	✓	