Prince Edward Island
Department of Health

Pharmaceutical Information Program Integration and Conformance Specification
FINAL

VOLUME 5 – Security

VERSION: 1.4.1 PRINTED 2006-12-19

TABLE OF CONTENTS

CHANGE LOG

Date	Version	Notes
May 19, 2006	0.1	Draft Template.
June 14, 2006	0.2	Draft.
June 26, 2006	1.1	FINAL.
September 15, 2006	1.3	Updated version number to 1.3.
November 1, 2006	1.4	Updated version number to 1.4.
December 18, 2006	1.4.1	Updated version number to 1.4.1

1 INTRODUCTION

The Prince Edward Island (PEI) Pharmaceutical Information Program (PhIP) Integration and Conformance Specification provides the necessary business and technical information required for application integration. This documentation set is composed of a series of volumes, which are intended for specific audiences.

There is a common set of volumes required by all software vendors. Two sets of business and technical volumes have been produced; one is intended for the practice of pharmacy while the other is intended for the practice of medicine. Interested parties may contact Sherry McCourt, Project Manager via telephone at (902) 368-6723 or via e-mail at samccourt@ihis.org to inquire about this documentation set or to request the most current version, and any technical questions may be directed to Patricia Holland, Technical Analyst at (902) 368-6194 or via e-mail at pmholland@gov.pe.ca.

1.1 Purpose/Audience

This specification is intended for software vendors, health care providers, health care professionals, and administrators who share responsibility for the implementation and operation of software that is capable of interacting with the PEI Pharmacy Network in a fully compliant manner.

This document describes the minimum implementation standards required for third-party provider software (local software) to be considered compliant with the functional requirements of the PEI Pharmaceutical Information Program as established by the Department of Health.

Local software applications must provide the ability for participating service providers (Providers) to perform the mandatory functions described herein. Communication by local software with the PhIP is conditional based on compliancy with the requirements described herein.

In addition to the provision of complaint software, Providers must ensure the following principles are established prior to implementing a “for production” Pharmaceutical Information Program connection:

- All users are provided adequate training in operating the compliant software;
- Privacy and confidentiality policies and procedures as outlined in the legislation and/or regulations are adhered to at all times;
- Proper telecommunications services have been acquired and are in accordance with the security requirements defined herein; and
- Adequate hardware and software infrastructure has been provided to users of the system.

1.2 Status of this Specification

This specification is in its final version.

1.3 Relationship to pan-Canadian Standards

The PEI Department of Health, in developing the PHIP, has endeavoured to adhere to nationally sponsored standards initiatives in all regards. Wherever possible, the standards, best practices, and processes agreed upon nationally have been adopted. Exceptions include where legislation, regulations, or mitigating factors have not made such possible. Instances where the Pharmacy Network has deviated from these standards are clearly identified.

The PEI Department of Health has worked in partnership with Canada Health Infoway in developing the Pharmaceutical Information Program.

Canada Health Infoway (CHI) is a not-for-profit organization made up of Canada's 14 federal, provincial, and territorial Deputy Ministers of Health. CHI was created in 2001 with the mandate to foster and accelerate the development and adoption of electronic health information systems in Canada. An important focus of CHI's investment strategy is to promote the creation and use of compatible standards and communication technologies on a pan-Canadian basis to support the implementation of interoperable systems across the country.

Canada Health Infoway's target is to have an interoperable electronic health record in place across 50 percent of Canada (by population) by the end of 2009. The route to this target is through the strategic investment of $1.2 billion.

A client registry (CR) is an essential component of any electronic health information system. A CR is a single directory that contains current patient identification information including Provincial Health Number (PHN) and demographics (name, address, date of birth, and gender). The CR also retains historic demographic information (maiden name and former addresses) which is critical to maintaining the concept of a lifetime record. The collection and retention of this information provides unique identification, which enables the linking together of all of the pieces of information that make up a patient's electronic health record.

CeRx is a pan-Canadian Clinical Drug Messaging Standard. This standard supports the clinical drug information interchange between and among clinicians. CeRx enables the population of the drug portion of the Electronic Health Records (EHR) at a provincial, territorial or regional level. These messages will allow the establishment of drug profiles within the EHR, as well as putting in place the workflows necessary to enable electronic prescribing.

The creation of a single pan-Canadian standard messaging specification aims at reducing costs for individual jurisdictions, software vendors and independent health care professionals in an effort to encourage adoption of these solutions and gain anticipated benefits.

NeCST is a National e-Claims Standard initiative whose goal it is to facilitate and support the development of a national electronic claims messaging standard for exchanging electronic health claims information across Canada. It will be used for private and public sector payors and for health service providers.

NeCST benefits to health care providers include:

- Ability to send electronic information to both private and public sector payors using the same message format;
- Efficiencies in electronic claims;
- Consistent format for all payors;
- Pan-Canadian standard across all jurisdictions; and
- Faster turnaround of claims processing and payment.

Benefits to the Pharmacy include:

- Ability to send more complete information, including compound components;
- Improved ability to bill for professional services against multiple plans from various insurers;
- Ability to send and receive more consistent messages and information from payors;
- Enhanced ability to electronically complete coordination of benefits (COB);
- Improved inventory control through the use of Universal Product Codes (UPC) and Global Product Identification Numbers (GPIN); and
- New messages allow pre-determination and electronic coverage extensions.

NeCST has been designed to facilitate all major health care business processes used to authorize, compile, submit, adjudicate and pay health care invoices submitted by any provider to any payor in Canada

In accordance with the jurisdictionally agreed collaboration process, this specification will be provided to the standards management groups and representatives from other Canadian jurisdictions to facilitate the highest level of consistency possible on a Pan-Canadian basis.

1.4 Volume Index

This PhIP Integration and Conformance Specification is composed of seven (7) volumes, each of which is described below.

1.4.1 Volume 1: Introduction

Volume 1 provides contact information, document formatting rules, and a description of the remaining volumes.

1.4.2 Volume 2: Business Rules

Volume 2 contains business rules based on the work processes that are to be supported within the practices of pharmacy and medicine. A separate document is provided for each practice area. It provides explicit business rules and implementation guidance as it will be supported within the jurisdictional PhIP.

1.4.3 Volume 3: Technical Rules

Volume 3 contains rules, work processes, and message sequences that are to be supported within the practices of pharmacy and medicine. A separate document is

provided for each practice area. It provides explicit technical rules and guidance to the intended jurisdictional Pharmacy Network implementation.

1.4.4 Volume 4: Message Catalogue

Volume 4 contains the complete list of message interactions and content/structure rules. In cases where a supporting standard exists, it will reference the standard and provide per-jurisdiction restrictions/constraints. In the case that the message is non-standard, complete interaction details will be included within this document. This includes information regarding the following:

- Network transmission and responses;
- Client Registry standard messages;
- Provider Registry standard messages;
- CeRx standard messages;
- NeCST standard messages;
- CPhA v3 standard messages;
- Custom messages; and
- Message formats and data definitions.

1.4.5 Volume 5: Security

Volume 5 contains a description of the security infrastructure, integration requirements, minimal security policies, and references to appropriate procedures and forms that must be completed as part of the integration process.

1.4.6 Volume 6: Glossary

Volume 6 contains definitions for all terms and acronyms used throughout the specification.

1.4.7 Volume 7: Supplementary Materials Catalogue

Volume 7 contains references, pointers, and descriptions of supplementary materials and other information sources considered relevant.

1.5 Document Conventions

The following conventions are used in each volume:

- ‘Must’, ‘Shall’, ‘Required’, ‘Minimum’, or ‘Mandatory’ indicate a mandatory requirement.

- ‘May’, ‘Should’, ‘Recommended’, ‘Optional’, or ‘Suggested’ indicate a functional ability that, while not required by a minimum implementation, should be considered.

- Acronyms are used throughout this document. The first use will typically include both the full name and the acronym. “Volume 6: Glossary” contains definitions of all acronyms used within the specification.

- Terms are used throughout this document. “Volume 6: Glossary” contains definitions of all terms used within the specification.

1.6 Related Standards/Documents

Please refer to “Volume 7: Supplementary Materials Catalogue”.

1.7 Disclaimer

All reasonable care has been taken by the PEI Department of Health to achieve accuracy throughout this specification. However, the PEI Department of Health cannot fully guarantee the accuracy of its contents. In reviewing this document, each party waives and releases the Province of Prince Edward Island to the full extent permitted by law from any and all claims related to the usage of material contained herein. In no event shall the Province of Prince Edward Island be liable for any incidental or consequential damages resulting from the use of these materials.

2 SYSTEM REQUIREMENTS

2.1 Business Overview

The local system will incorporate an effective security scheme that will:

a) Control system access;

b) Uniquely identify each authorized Provider;

c) Require Provider authentication for system access;

d) Provide anti virus and where possible firewall services; and

e) Provide encryption capabilities where required.

2.2 Business Rules

1. Physical and logical controls must be placed on the local system to restrict access to all system components to only those individuals who actually require access to that part of the system as part of their job.

The intent of these controls is to prevent unauthorized systems access by:

- Restricting the access of Providers to only those parts of the system they have a need to use;
- Providing unique identification for each authorized Provider thereby enabling a detailed audit trail of every PhIP transaction; and
- Providing strong user authentication processes (e.g., passwords).

2. The local software must restrict a User ID's access to authorized business functions regardless of physical location within the building**.** For example, a clerk who has access to the local computer system(s) must not be able to sign on to the pharmacy system and gain access to confidential patient data.

2.3 Local System Provider Authentication

2.3.1 User IDs

1. Unique User IDs must be assigned to each individual who requires access;

2. Individual Providers must assign a unique password to their User ID;

3. User IDs must be authorized to access an authorized set of system functions (e.g., filling prescriptions, stock control, etc.);

4. User IDs must not be shared. To ensure individual accountability, each User ID is to be assigned to a single person who is accountable for all activities of that User ID;

5. The local system must place a User ID in a revoked status after a maximum of five (5) consecutive failed sign on attempts. Initialization of the User ID requires intervention of the manager or system administrator with a higher level User ID;

6. A high level User ID must be defined to control security access and other restricted system functions. This User ID's functionality must not include the ability to process PhIP transactions; and

7. The software must have functionality to revoke or disable User IDs.

2.3.2 Passwords

1. Each Provider must be able to set their own password;

2. Providers must be instructed not to share passwords with other Providers or managers;

3. A security application must force Providers to set a new password after a password has been reset or a new User ID is assigned;

4. Passwords must be stored by the local system in an encrypted file that cannot be read;

5. Password characters must not be displayed on monitors when entered;

6. Passwords must not be hard coded into any system file or routine and must be keyed in by the Provider each time the Provider signs on;

7. The local system must:

    a) Force the use of passwords at least 6 characters long;

    b) Force the Provider to change passwords within 90 days; and

    c) Prevent immediate reuse of a password.

8. When the password expires the Provider should be advised by the local system and instructed (forced) to immediately assign a new password. The system does not need to lock out the Provider because the password has expired.

2.3.3 Other Authentication Methods

Alternative forms of Provider authentication such as swipe cards or biometrics may be used in the place of passwords. If swipe cards are used to authenticate system access:

1. Providers who have been issued cards must keep the cards on their possession or control at all times; and

2. The head of the local organization must ensure that procedures for the secure storage of un-issued swipe cards are in place and are being followed.

2.3.4 Remote Access to Local System

All remote access to the local system must:

- Use a cryptographic tunnelling protocol to provide confidential, sender authentication, and message integrity to achieve intended privacy; an IPSec VPN or a clientless SSL VPN (Medical Practitioner's only) are suggested by the Department; and
- Carry a digital certificate from the Island Health PKI to authenticate the server.

2.3.5 Pharmacy TCP/IP Access

The PEI Department of Health will be implementing IPSec VPN connections with PEI pharmacies. Some pharmacies will require a dedicated tunnel from their existing firewall to the IHIS firewall. For other PEI pharmacies, the implementation requirement is a VPN edge device at the pharmacy site.

IPSec VPN uses cryptographic tunneling protocols to provide confidentiality, sender authentication, and message integrity to achieve the intended privacy. IPSec VPN is essentially a firewall-to-firewall secure connection.

The IPSec VPN solution ensures total privacy and protection of the sensitive health information that will be transported over the connections.

With this approach, computers behind the remote firewall do not need any special software because the secure IPSec VPN tunnel is negotiated and maintained by the two firewalls.

2.3.6 Medical Practice TCP/IP Access

The PEI Department of Health will be implementing a clientless SSL VPN solution for remote connectivity from Medical Practitioner's offices.

This solution permits the virtualization of a remote access deployment by logically separating distinct groups within a single physical SSL VPN infrastructure. The SSL VPN infrastructure will allow IHIS to separate organizational entities and business partners by defining unique networks (portals), security features (endpoint, authentication, authorization and auditing) and management policies on a customer or group basis.

Two-factor authentication is also necessary for Clientless SSL VPN.

2.3.7 Encryption of Data

All health data traffic must be encrypted when:

1. The data is transmitted beyond a single physical network;
2. The network connections are between two or more IHIS participants; and
3. The network is shared by more than one business entity.

The encryption method used must comply with the following standards:

1. Secure Sockets Layer V3 (SSL); and
2. Transport Layer Security V1 (TLS).