



PharmaNet

Professional and Software Compliance Standards

Volume 5 – Security

Version 3.1

November 2004

DOCUMENT MODIFICATION HISTORY		
VERSION	RELEASE DATE	DESCRIPTION
2.5		Previous single document
3.0	April 2001	Split form full source document to individual sections
	August 2002	Completed source document split
	April 2003	Correction to document format
	June 2003	Updated transaction descriptions
	July 2003	Spelling corrections and minor wording changes
	October 2003	Removed Caveat and corrected footnotes
3.1	November 2004	Updated spelling of <i>healthnetBC</i>

CONTENTS

1	GENERAL INFORMATION	3
1.1	THE VOLUMES	3
1.2	THE AUDIENCE	4
1.3	THIS DOCUMENT	4
2	SYSTEM REQUIREMENTS	5
2.1	BUSINESS OVERVIEW	5
2.2	BUSINESS RULES	5
2.3	LOCAL SYSTEM PROVIDER AUTHENTICATION	6
2.3.1	<i>User IDs</i>	6
2.3.2	<i>Passwords</i>	7
2.3.3	<i>Other Authentication Methods</i>	8
2.3.4	<i>Remote Access to Local Systems – Dial Access</i>	8
2.3.5	<i>PharmaNet Committee Endorsement</i>	8
2.3.6	<i>Hospital Emergency Departments</i>	8
2.3.7	<i>Internet Access</i>	9
2.3.8	<i>healthnetBC Access Control</i>	10
2.3.9	<i>Encryption of Data</i>	10

1 GENERAL INFORMATION

The Professional and Software Compliance Standards Document for PharmaNet has been revised into volumes, divided by PharmaNet participant functionality requirements.

The 'library' approach provides more logical formatting while reducing redundancy and repetition.

There are common volumes required by all software developers and both business and technical volumes for the different functions. This enables software developers to download only the necessary volumes. The documentation is available on the *healthnetBC* Products and Services Catalogue web site. <http://healthnet.hnet.bc.ca/catalogu/index.html>

1.1 The Volumes

The 6-volume documentation set contains:

Volume 1 – Introduction

Volume 1 introduces the reader to common development components, such as:

- Document Conventions and Structures
- Related Standard
- Contacts
- Support Responsibilities
- Compliance Evaluation Process
- Mandatory policies and procedures to ensure compliance with all standards.

Volume 2 – Business Rules

Volume 2 has been further divided into separate documents for the functionality requirements of Hospital Admitting (HA), Emergency Department (ED), Medical Practice (MP), and Pharmacy access.

This volume contains the *implementation requirements* and the *business rules* related to the use of the available transactions and the local system requirements.

Volume 3 – Technical Rules

Volume 3 has been further divided into separate documents for the functionality requirements of Hospital Admitting (HA), Emergency Department (ED), Medical Practice (MP), and Pharmacy access.

This volume contains the *general processing* and the *technical rules* related to the use of the available transactions and the *local system requirements*.

Volume 4 – HL7 Message Catalog

Volume 4 identifies transaction details and message responses, such as:

- Network Transmissions and Responses
- Health Level 7 (HL7) Standards
- Message Formats and Data Definitions
- Input and Output Message Segments and Fields

Volume 5 – Security

Volume 5 provides security objectives, requirements and guidelines and a framework for developing policies and implementing local security controls.

Volume 6 – Glossary

Volume 6 lists a glossary of terms persistent through out *healthnetBC*.

1.2 The Audience

The compliance standards documentation is intended for software developers, health care Providers, administrators and other health care professionals who share responsibility for implementing compliant software in their organization.

1.3 This Document

This volume is shared by all the *healthnetBC* participant functionalities. It describes the security measures required to access *healthnetBC* and the security that must be implemented at the client's source.

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.

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:

- a) Restricting the access of Providers to only those parts of the system they have a need to use
 - b) Providing unique identification of each authorized Provider thereby enabling a detailed audit trail of every *healthnetBC* transaction
 - c) 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 hospital admitting clerk with access to non-sensitive data on *healthnetBC* must not be permitted to sign on to a pharmacy system which would permitting access to confidential *healthnetBC* 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. Where technically possible, the sending system must have a feature that clears the screen of personal and confidential information when a *healthnetBC* session has been inactive for more than 15 minutes. Two examples are locking screensavers and automatic disconnection of inactive sessions. The screen must remain clear of personal and confidential information until an authorized Provider successfully enters a valid User ID and password.
6. The local system must place a User ID in a revoked status after 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.
7. 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 *healthnetBC* transactions.
8. 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 must¹:
 - a) Force the use of passwords at least 6 characters long
 - b) Force the Provider to change passwords within 42 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.

¹ Currently under review for software which does not access confidential PharmaNet data.

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
2. The head of the local organization must ensure that procedures are in place to securely store un-issued swipe cards.

2.3.4 Remote Access to Local Systems – Dial Access

All dial access to local systems must:

1. Be approved by the head of the local organization
2. Provide access and security controls equivalent to the controls required above
3. Provide encryption of sensitive data.

2.3.5 PharmaNet Committee Endorsement

The PharmaNet Committee endorses the recommendations that:

1. The local modem should be turned off when not in use
2. Modems with password prompts should be used
3. Dial back modems should be used in order to decrease the risk of exposure to local patient records. CPBC

2.3.6 Hospital Emergency Departments

The use of remote access software is not permitted for hospital emergency departments except by an SSO for the purpose of supporting the software.

2.3.7 Internet Access

All Internet access from local systems must:

1. Be approved by the head of the local organization
2. Provide access and security controls equivalent to the controls required above; and,
3. Provide regular (preferably daily) audit reports of failed accesses to facilitate follow up of attempted or potential system intrusions.

Current policy will allow the local system to access the Internet and hence their SSO and other organizations on the Internet. The default configuration of the *healthnetBC* participant router will be to place no restrictions on either inbound or outbound traffic to the Internet. If a Provider has security concerns with this configuration, they may request implementation of a firewall. The Provider must specify which IP addresses they wanted to be able to communicate with and all others would be blocked by the firewall.

The use of firewalls on the local computer are endorsed and encouraged by the PharmaNet Committee and the CPBC. CPBC

Implementing a firewall scheme requires a Telecommunication Service Request (TSR) submitted by the MOHS PharmaNet contact on behalf of the Provider. An additional TSR would be required if the Provider wanted to change that scheme at a later date. TSRs cost \$50.00 each and are payable by the Provider to the Minister of Finance.

2.3.8 *healthnetBC* Access Control

To provide transaction audit ability and accountability the local system must ensure that the *healthnetBC* transaction appropriately identifies:

1. The person initiating the transaction (e.g., a user of a Hospital Admitting system).
2. The person responsible for the transactions (e.g., the 'pharmacist' on pharmacy transactions; the 'responsible physician' for Emergency Department transactions, etc.).
3. Identification must be based on a positive action by the Provider. Examples of positive action are:
 - a) Card swipe
 - b) Entry of password or User ID or equivalent

When the initiating or responsible Provider performs a transaction change, the user identification on the transaction changes.

2.3.9 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 *healthnetBC* participants
3. The network is shared by more than one business entity.