BRITISH COLUMBIA

**Ministry of Health Services**

## Professional and Software Compliance Standards For HL7 Messaging

# Volume 2 – Compliance Process

Version 2.1

November 21, 2003

| | |
|---|---|
| **Author:** | *health*netBC |
| **Creation Date:** | September 30, 1999. |
| **Last Updated:** | December 11, 2003 |
| **Document Number:** | |
| **Version:** | 2.1 |

# Approvals:

| **Project Sponsor** | | |
|---|---|---|
| | Signature | Date |
| **Kathy Hill** | | |
| *health*netBC Access Services | | |

| **Compliance Process Standards** | | | |
|---|---|---|---|
| | **Approval** | | **Reviewer** |
| Signature: | | Signature: | |
| Name: | **Kathy Hill** | Name: | **Tony Stehle** |
| Title: | Manager<br>*health*netBC Access Services | Title: | SSO Coordinator<br>*health*netBC Access Services |
| Date: | | Date: | |

# Contents

# 1 General Information

This document and its companion volumes contain the **Professional and Software Compliance Standards for HL7 Messaging** between the BC Ministry of Health and external clients. These standards are used for the exchange of information with various business areas within the Ministry including: the Client Registry (patient/client demographics), MSP (beneficiary coverage), MSP Employer Services (enrolment of employees and dependants), Primary Health Care (patient rostering) and Continuing Care (client demographics and history).

## 1.1 What are the volumes in this set?

The HL7 Standards for messaging to and from BC Ministry of Health applications are described in a series of business and technical volumes.

Volume 1 – Introduction to the Professional and Software Compliance Standards. A general introduction to the specifications along with tabular listings of all supported messages and message interactions.

Volume 2 – The evaluation process to determine if software is compliant with the Ministry's standards, as described in these documents

Volume 3 – Separate publications containing the business rules for each particular business area. (3a – Client Registry, 3b – MSP Direct are available to date)

Volume 4 – HL7 Message Specifications. A series of standalone documents for each of the transactions used by the BC Ministry of Health.

Volume 5 – Network Transmissions

Volume 6 – Security

Volume 7 – Glossary

All documentation is available on the *health*netBC Products and Services Catalogue web site http://healthnet.hnet.bc.ca/catalogu/tech/compdocs.html

## 1.2 Corrections and updates

Corrections and update notes can be found at the end of this document. A vertical line in the outside border denotes corrections within the document. [1]

## 1.3 Who is the audience?

This document is intended for use by:

a) Software Support Organizations (SSO) who wish to develop software that is compliant with the BC standard for the exchange of Client Registry data and other Ministry supported transactions.

b) Providers, administrators, health care professionals and MSP Benefits administrators (public and private employers) who are responsible for the implementation of compliant software in their organizations.

## 1.4 Contacting Technical Support

### 1.4.1 Technical Support

a) Software Compliance Standards

b) Compliance Evaluation Scheduling;

c) Access to software development, testing, production & training databases;

d) Business Development Team

e) Requests for documentation, bulletins, etc.

f) Technical support for HNSecure/Infrastructure

g) Post-implementation support

The Software Support Organization Coordinator is the first point of contact in the Ministry of Health for technical software development support.

Email: HLTH.HnetSSOSupport@gems3.gov.bc.ca

Telephone: (250) 952-3531

### 1.4.2 Connections Support

A *health*netBC Access Services Connections Coordinator will assist with connecting *health*netBC compliant software to access *health*netBC data.

Email: HLTH.HnetConnection@gems1.gov.bc.ca

### 1.4.3 Help Desk

Reference is made in some transaction business rules that participants are required to contact the *health*netBC Help Desk to resolve issues. The *health*netBC Help Desk line is NOT the first contact point for Vendors.

The *health*netBC Help Desk is available 24 hours per day, 7 days per week to accept, log and resolve problems. The level of support may be limited outside of regular business hours.

If calling from Vancouver / lower mainland:

(604) 682-2316

If calling from Victoria:

(250) 952-2293

If calling from elsewhere in BC:

Toll Free 1-888-764-2323

# 2 Compliance Parameters

The Ministry's Software Support Organizations (SSO) Coordinator and the Quality Assurance Staff perform compliance evaluation where appropriate.

The evaluation is to determine that the sending system software complies with all the requirements stated in this document and that all functions and processes of the sending system provide accurate results. Both constructive and destructive testing is performed.

All aspects of *health*netBC functionality available on the sending system software will be tested regardless of use at the testing location.

This volume is the basis for establishing evaluation parameters. Compliance testing documentation is available on the *health*netBC web site.

## 2.1 Release Management

The following requirements for release management apply to all *health*netBC compliant software, including the HNSecure security toolkit if an SSO has recompiled and/or altered the HNSecure toolkit as supplied by the Ministry.

Written notification to the SSO Coordinator describing changes or upgrades to the sending system software is required before SSOs may release the changes to production clients.

The SSO Coordinator will have the option of evaluating any release of sending system software before it is put in a production environment on *health*netBC. Evaluation facilities will be provided by the SSO for all compliance evaluations. Evaluation dates will be scheduled by mutual agreement.

An SSO may be exempted from a compliance evaluation at the discretion of the SSO Coordinator if functionality accessing *health*netBC is not affected. The SSO must submit written documentation identifying the following information before exemption will be considered.

a) Purpose of the change

b) Description of change and/or functionality

c) Anticipated impact on *health*netBC data and/or transactions

d) Version number

e) Anticipated release date

Requests for changing software version numbers will be accepted from either the manager at the client site or the SSO and must be in writing (fax or e-mail). A telephone request will require a follow-up fax or e-mail.

Quality Assurance will keep the Help Desk advised of all compliant versions for each SSO.

## 2.2 Version Control

A version number must uniquely identify each version of the sending system software that has been proven compliant. This version number must be in each transaction on the ZHD segment for all inbound transactions. Audits will be done to ensure that the version number being transmitted correlates to the version that was approved during the compliance evaluation. The sending system software version number must increment when a major new release is issued.

## 2.3 Emergency Upgrades

If emergency changes to compliant software must be performed to sending system software, notification of the changes must be provided in writing to the SSO Coordinator by the following working day.

The notification must identify:

a) Installation date

b) Affected sites

c) Reason

d) Description of software changes

e) Impact assessment.

The SSO Coordinator will determine the need for a compliance evaluation.

## 2.4 Compliance Evaluation Process

The following is a general description of the compliance evaluation process and may be subject to change.

1. After an SSO has successfully tested their software and is satisfied their program is working according to specifications, they must contact the SSO Coordinator to schedule a compliance evaluation. A mutually agreeable evaluation date will be scheduled. Questions regarding the compliance evaluation process should be directed to the SSO Coordinator.

2. All compliance evaluations will be held in British Columbia at a mutually agreed location. If an SSO wants a compliance evaluation held at an out of province location a written request must be submitted to the SSO Coordinator at least one month prior to the anticipated evaluation date.

3. Unless specifically requested and agreed to, all requirements as outlined in the Compliance Specifications document will be evaluated.

4. The compliance team will supply the SSO with a list of data required for the evaluation. It is recommended that the SSO incorporate this data on their sending system prior to the evaluation.

5. The *health*netBC compliance team will instruct and observe the transmission of transactions to the Ministry test databases. Each transaction will be verified against a set of expected results. Where applicable, the compliance team may examine the sending system to determine what *health*netBC data is being stored on the sending system.

6. When the evaluation has been successfully completed, the compliance team will record details of the SSO software including version, date, and file size(s).

7. If a sending/receiving system fails, the evaluation may be halted. If the compliance testing team is on-site, they may depart and a new evaluation will be scheduled when the SSO believes the problem rectified. The compliance testing team is not required to remain on site while debugging is undertaken.

8. A written evaluation report will be provided to the SSO no more than five business days following the evaluation. This report will detail all deficiencies and corrective actions required or provide approval for distribution to clients.

9. The compliance evaluation process may take up to 3 consecutive days. Evaluations will take place during normal business hours, Monday through Friday.

10. Sending/receiving system software that includes HNSecure, the *health*netBC security protocol, will be tested to determine if HNSecure has been altered or compiled for a different environment. If it has, there will be compliance tests performed specific to HNSecure.

11. Prior to compliant software being installed for production use, the SSO must sign a Service Level Agreement with the Ministry and a confidentiality agreement with the client.

## 2.5 Charges And Penalties

### 2.5.1 Compliance Evaluations

For each software release, the compliance team will be available at no cost to the SSO to a maximum of one compliance evaluation (3 days) and one follow up evaluation (3 days), otherwise, the SSO will be responsible for wage and travel costs of the compliance team.

When additional evaluation dates are required, the SSO must provide a written request to the SSO Coordinator. Requests are subject to Ministry management approval. Travel costs, wages and other out-of-pocket expenses for members of the compliance team may be the responsibility of the SSO for additional evaluations. Out of province compliance evaluations must be funded by the SSO.

For SSO funded compliance evaluations, statements of expenses and receipts will be provided for the amount payable; if required. Payment must be received no more than 2 weeks following the completion of the compliance evaluation.

### 2.5.2 Penalties

If non-compliant software is released for production use, SSOs may be instructed to remove the non-compliant version.

If the installation of non-compliant software results in a system error or failure (i.e. time-outs, table corruption, etc.), the SSO will be responsible for the cost of resources required to rectify the situation.

Other penalties include the immediate termination of access to *health*netBC services and telecommunications facilities and, where applicable, referral to the appropriate regulatory body for investigation and disciplinary action.

## 2.6 Compliance Audits/Inspections

A team with representatives from the Ministry reserve the right to perform random, unannounced audits/inspections at client sites. The purpose of an audit / inspection is to determine if the client is in compliance with the software and professional standards as described in this document.

### 2.6.1 Client Sites

The manager at the client site will be given a deficiency report by the audit team and will be required to have the software and procedural deficiencies corrected within a specified period of time. In situations where the deficiencies are not corrected by the deadline, a report may be forwarded to the Ministry and/or the regulatory body for review.

## 2.7 Requirements To Connect To *health*netBC

It is the responsibility of the client or the SSO to ensure the sending system including cabling, hardware, software and local area network is working properly. Services such as firewall schemes, network connections, modems, monitors, and registered IP must be arranged and paid for by the client or SSO.

In order to communicate with the Ministry, each transmitting PC must be connected to the Internet. The PC must have TCP/IP software and a connection to a router which itself is connected to the Internet. This may be achieved by connecting the PC to the local area network (LAN) that has a connection to the router, or by dial-up access. If the router being used is not an approved B.C. Government router, the sub-domain name or the IP address range for the site must be communicated to the SSO Coordinator to ensure site access is enabled.

If the ISP does not assign the IP address, it must be registered with the Internet Assigned Number Authority at http://www.iana.org/

Refer to Volume 6 – Security for additional information about connecting with the Ministry.

Workstations must have access to the World Wide Web and have the following level of browsers:

- Internet Explorer Version 5.5 (or later) with 128-bit encryption.
- Netscape Navigator Version 4.5 (or later) with 128-bit encryption

The Ministry supports test and training environments during business hours (8 a.m – 4:30 pm, Pacific Time, Monday to Friday).

- The Testing environment is reserved for software compliance testing only.
- The Training environment is used for training clients and end users after the software has successfully passed the compliance evaluation.

# 3 Implementation Requirements

## 3.1 Hospital Admitting

In order for *health*netBC participants to obtain access to *health*netBC data:

### 3.1.1 Agreements

1. For hospitals, the CEO (or designate) of the Health Authority must sign and submit a Data Access Agreement and a Confidentiality Undertaking Agreement with the Ministry. These agreements include items such as:
    - Permission to conduct spot audits/inspections by the *health*netBC compliance team;
    - Administration and maintenance of operator Ids;
    - Penalties for misuse of information;
    - Problem escalation procedures (i.e., identification of key personnel);
    - Contact information.
2. *health*netBC participants must obtain signed confidentiality undertakings from all employees accessing confidential *health*netBC data and maintain a copy with the personnel files.

### 3.1.2 Software and Training

1. *health*netBC participants must install *health*netBC compliant software. A list of compliant SSOs is available from the SSO Coordinator. See "Contacting Technical Support" .
2. Designated staff must receive training/education on use of sending system software from the SSO supplying the software.

### 3.1.3 Connections

1. Questions regarding specific connection requirements and procedures can be directed to the Connections Coordinator. See "Contacting Technical Support".

## 3.2 Hospital Emergency Department

In order for physicians in emergency departments to obtain access to *health*netBC data:

### 3.2.1 Agreements

1. The CEO (or designate) of the Health Authority must sign and submit a Data Access agreement and a Confidentiality Undertaking agreement with the Ministry. These agreements include items such as:

   - Permission to conduct spot audits/inspections by the *health*netBC compliance team; administration and maintenance of operator Ids;
   - Penalties for misuse of information;
   - Problem escalation procedures (i.e., identification of key personnel);
   - Contact information.

2. The hospital CEO and the Chief of the hospital ED must sign an undertaking acknowledging responsibilities related to confidentiality for ED physicians and hospital staff.

3. Hospital administration must obtain signed confidentiality undertakings or pledges from all employees accessing confidential *health*netBC data and maintain a copy on file. Refer to "Available documentation".

### 3.2.2 Software and Training

1. Hospitals must install *health*netBC compliant software. A list of compliant SSOs is available from the SSO Coordinator. See "Contacting Technical Support".

2. Physicians and/or designated support staff must receive training/education on use of sending system software from the SSO supplying the software.

### 3.2.3 Connections

1. Questions regarding specific connection requirements and procedures can be directed to the Connections Coordinator. See "Contacting Technical Support".

## 3.3 Medical Practice

In order for a medical practice to obtain access to *health*netBC data:

### 3.3.1 Agreements

1. The designated physician in the medical practice must complete a Data Access agreement and a Confidentiality Undertaking agreement with the Ministry.

2. The designated physician must complete an undertaking that confirms that all security and confidentiality provisions of *health*netBC and the CPSBC have been satisfied.

3. Each individual (including physicians, locum physicians, nurses and medical office assistants) in the medical practice authorized to access *health*netBC must sign a confidentiality undertaking or pledge. Refer to "Available documentation".

4. The designated physician must complete a confidentiality agreement with the SSO providing the software.

### 3.3.2 Software and Training

1. The medical practice must install *health*netBC compliant software. A list of compliant SSOs is available from the SSO Coordinator. See "Contacting Technical Support".

2. Individuals in the medical practice who are authorized to access *health*netBC must receive training/education on the use of the sending system software, the business, privacy and confidentiality standards and the policy and procedures developed by the medical practice for access to *health*netBC.

### 3.3.3 Connections

1. Questions regarding specific connection requirements and procedures can be directed to the Connections Coordinator. See "Contacting Technical Support".

## 3.4 MSP Direct for Employers

In order for an employer to obtain access to MSP Services:

### 3.4.1 Agreements

1. The CEO of the *health*netBC participant must sign and submit a Data Access agreement and a Confidentiality Undertaking agreement with the Ministry.

2. When the sending system software is supplied by an SSO other than the Ministry, the CEO must sign a confidentiality agreement with the SSO.

3. The *health*netBC participant must designate an individual to be responsible for ensuring all security and confidentiality provisions of *health*netBC are satisfied on an ongoing basis.

4. If applicable, the participant must inform the Ministry of changes in staff authorized to access *health*netBC data, and their related user ID.

5. Each employee authorized to access *health*netBC services must sign a confidentiality undertaking. Copies of these undertakings must be available for inspection by the *health*netBC compliance team. Refer to “Available documentation”.

### 3.4.2 Software and Training

1. The *health*netBC participant must install *health*netBC compliant software. A list of compliant SSOs is available from the SSO Coordinator. See “Contacting Technical Support”.

2. Each employee authorized to access *health*netBC services must receive training/education on the use of the sending system software as well as the functions and features pertaining to the messaging standard, from the SSO supplying the software.

### 3.4.3 Connections

1. Questions regarding specific connection requirements and procedures can be directed to the Connections Coordinator. See “Contacting Technical Support”.

## 3.5 HNSecure

In order for *health*netBC participants to use HNSecure to access *health*netBC data the participant must:

### 3.5.1 Software and Training

1. Install *health*netBC compliant software. A list of compliant SSOs is available from the SSO Coordinator. See “Contacting Technical Support”.

2. Receive training/education on use of features relating to HNSecure security. The pertinent details can be found in Volume 6 - Security.

### 3.5.2 Connections

1. Register a public key with *health*netBC for each Network-Facility-ID, and;

2. Password protect the matching local "private key" in the sending system.

# 4 Ministry Support

## 4.1 The Ministry maintains:

a) Ongoing application test environment

b) HNSecure test environment

c) Ongoing training environment

d) Network management

e) Compliance standards and evaluation schedule

f) Transaction structure definitions

g) SSO Coordinator support

## 4.2 Ministry SSO Coordinator

The Software Support Organization Coordinator is the first point of contact in the Ministry of Health for technical software development support.

Email: HLTH.HnetSSOSupport@gems3.gov.bc.ca

Telephone: (250) 952-3531

## 4.3 Available documentation [2]

### 4.3.1 *health*netBC BC Web Site

Access the *health*netBC web site at: http://healthnet.hnet.bc.ca

The *health*netBC BC web site includes an Overview to *health*netBC BC, its Mission Statement and Objectives.

### 4.3.2 *health*netBC Compliance Standards

Copies of this and related volumes for the Professional and Software Compliance Standards are available on the web site http://healthnet.hnet.bc.ca/catalogu/tech/compdocs.html.

Note that there are also compliance documents for the PharmaNet Standard. These standards are similar but not interchangeable.

### 4.3.3 Web Services User Support Documentation

The following downloadable documents are on the Health Registration Website: http://healthnet.hnet.bc.ca/catalogu/healthreg/phnassign.html

*Access Administrators Guide*

- This document provides information and procedures for coordinating all user access to *health*netBC/BC Web Business Services.

*Working on the Web – A Guide for New Users*

- This guide has been developed to show new users how to access and work with the *health*netBC/BC Web Business Services.

*Introduction to health*netBC*/BC Web Business Services Demonstration Package*

- This demonstration package provides a quick overview of the functionality offered by *health*netBC/BC Web Business Services. This sample set is intended for prospective new clients interested in getting a look and feel of the business services and assumes familiarity with web browsers.

*Health Authority User Guide*

- This document is intended for Health Authorities authorized to use *health*netBC/BC Web Business Services. This user guide outlines the Eligibility, Demographics and PHN Assignment business services, describes the processing requirements of each business service, provides business rules, and describes results.

*MSP Direct – Employers User Guide*

- This document is intended for Employers authorized to use *MSP Direct Web Business Services*. This user guide outlines new Employer Business Services, describes the processing requirements of each business service, provides business rules, and describes results. This guide is available on http://healthnet.hnet.bc.ca/catalogu/healthreg/mspcover.html. This guide is to be used in conjunction with the *Health Authority user Guide*.

### 4.3.4 Document Attribute Dictionary (DAD)

For each type of document used for recording information in Maintain/Trusted Evidence Transactions, the DAD contains details for mandatory and optional data entry. Information on the structure of the DAD is in Appendix E of these documents. The DAD file (MS Word document) can be down loaded from the Compliance Standards Documentation website, http://healthnet.hnet.bc.ca/catalogu/tech/compdocs.html.

### 4.3.5 Confidentiality Undertaking

Private and public organizations wishing to access *health*netBC must have in place a policy regarding security safeguards for patient/client information

obtained/used by employees. Only those individuals who sign a Confidentiality Undertaking will be allowed access to *health*netBC products and services.

The policy/confidentiality undertaking refers to the authority on which the pledge is based:

- Public organizations must adhere to the *Freedom of Information and Protection of Privacy Act* and the organization's (e.g. hospital) policy;
- Private organizations must adhere to the *Medicare Protection Act* and/or the Medical Practice policies.

### 4.3.6 Professional and Software Compliance Tests

The following downloadable files are on the Compliance Standards Website:

- Software Support Organizations Development Test Scenarios for Health Service Providers
- Software Support Organizations Development Test Scenarios for Employers

### 4.3.7 HNSecure Documentation

The following documents are available on the HNSecure website:
http://healthnet.hnet.bc.ca/catalogu/phase3/index.html

*HNClient & HNServer Technical Specifications*

- HNClient sends HL7 messages to a server facility for processing and waits for a response. In order to facilitate this there are three major client application interface methods: HNAPI, HNClient, and HNLLI. The first section of this document describes the HNAPI portion of the library, followed by HNClient, and then HNLLI. While applications may use any one of these for secure communications, the HNClient and HNAPI interfaces are the easiest and the most flexible.

*HNClient & HNServer Business Specifications*

- This document describes the functional characteristics of the facilities a client application may make use of and how to go about using them when communicating with HNGATE or other Ministry of Health application servers/databases. It includes specifications for HNAPI, HNClient, HNLLI, HNSETUP, HNServer and HL7XFER. The sample applications provided to demonstrate use of these facilities are also described.

*Application Services Professional and Software Compliance Standards HNSecure - health*netBC*/BC Security Protocol*

- Refer to Volume 6 - Security for the latest Security standards.

*HNSecure Application Developer's Guide*

- This document was written to assist software developers involved in developing *health*netBC/BC client applications using the libraries and routines provided in the HNAPI/HNClient/HNServer Toolkit and sample programs.

*How To Set Up and Use HNSecure (for Software Developers)*

- This document is a quick reference guide for application developers using HNSecure. It provides a step-by-step guide for setting up HNCLIENT.

*HNSecure Compliance Tests*

- This document is found on the Compliance website
- It describes the compliance evaluation for the standards and rules that pertain to the Ministry's security protocol, HNSecure. This document assists Software Support Organizations (SSOs) to understand and pass an HNSecure compliance evaluation. Each compliance test that will be performed to ensure that the HNSecure portion of an SSO's application conforms to the Ministry's security standard is described.

### 4.3.8 HNSecure Developers Toolkit

The HNSecure Developers Toolkit is available from *health*netBC s to either incorporate into sending system software, or to use as sample code.

The HNSecure Toolkit contains executable programs, source code and sample programs that can be used as templates as well as Certicom Libraries. The toolkit consists of sample programs that provide sending system software with an interface routine, a network gateway and security services, including transaction encryption/decryption and authentication of network end points.

Registration is required as part of the licensing agreement for distribution of the Certicom Libraries. The HNSecure ToolKit Registration website is http://healthnet.hnet.bc.ca/catalogu/phase3/toolkit.html.

# Document History

| DOCUMENT MODIFICATION HISTORY | | |
|---|---|---|
| Version | Release Date | Description |
| 2.0 | September 1999 | Original single document |
| 2.1 | November 21, 2003 | • New publication as single volume.<br>• Added new General Information and Updated contacts, links and documentation resources<br>. |
| | | |

[1] 02/Nov/27 – example of correction
[2] The Health Registry Procedure Guide from HRS v2.0 has been discontinued.