BRITISH COLUMBIA

Ministry of Health Services

College of Pharmacists of
British Columbia

Professional and Software Compliance Standards For HL7 Messaging

Volume 6 - Security

Version 3.0

November 21, 2003

Author:	*healthnetBC*
Creation Date:	September 30, 1999
Last Updated:	December 19, 2003
Document Number:	
Version:	3.0

Approvals:

Project Sponsor		
	Signature	Date
Kathy Hill Manager - *healthnetBC* Access Services		

Compliance Process Standards			
	Approval		**Reviewer**
Signature:		Signature:	
Name:	**Colin Booth**	Name:	**Doug Williscroft**
Title:	Manager, Information Management Security	Title:	ESD Architect, IMG, Standards & Architecture
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 and Data Integrity

Volume 7 – Glossary

All documentation is available on the *healthnetBC* 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 Margins 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) '*health*netBC participants' (aka 'participants') – organizations that access *health*netBC information resources. This includes healthcare providers, healthcare administrators, health care professionals and MSP Benefits administrators (public and private employers) who are responsible for the implementation of compliant software in their organizations.

2 Overview

This volume contains security objectives, requirements and guidelines for users and participants of *health*netBC. It provides a framework for developing and implementing local policies and security controls. It includes security specifications for Software Support Organizations (SSO) to incorporate into software accessing *health*netBC services.

For the purposes of this document, computing processes that connect to *health*netBC resources are called **sending systems**. The primary focus of this set of compliance documents are systems that connect via HL7 message protocols, but the security principles apply to sending systems that may use other protocols.

2.1 Security Context

This volume is concerned with security controls applied to computing processes that connect to *health*netBC information resources. Within this, there are two security contexts of specific concern, distinguished from each other by how end users connect to the computing process:

1) Connection over 'trustworthy' networks – that is, over networks falling entirely under that administrative control of a single organization and over which the *health*netBC participant organization has direct or contractual influence such that system interactions on the network are not visible to other participants in the network; and

2) Connection over untrustworthy networks, such as the Internet.

This distinction has particular consequence to user authentication.

The connection between sending systems and *health*netBC is via *health*netBC's HNSecure, a protocol, which provides secure transport for HL7 transactions and binary

files attached to HL7 transactions over IP networks. HNSecure is described later in this volume.

3 Purpose

Security controls are intended to ensure, enable and provide mechanisms to protect the confidentiality, integrity and availability of information and information systems. The controls required or recommended in this volume support business processes while providing a framework consistent with legislated requirements and industry best practices.

The other volumes of the Software Compliance Standards contain business rules that have security implications. Every effort has been made to ensure the requirements in this volume are consistent with the intent of the business rules stated elsewhere in *health*netBC Software Compliance Standards. Questions or requests for clarification of security requirements should be directed to *health*netBC (see Volume 1 - Contacts).

The requirements of this section are minimum requirements. *health*netBC participants are free to implement more stringent requirements to meet local business needs.

Conventions used in this volume:

The word ‘must’ indicates a mandatory requirement.

The word ‘should’ indicates a recommended practice or process.

The word ‘could’ indicates an alternative that *health*netBC participants may wish to consider to improve their security practices.

4 Security Objectives

Security objectives are intended to:

- Enable compliance with Freedom of Information and Protection of Privacy Act and any other applicable legislation or regulation;
- Provide a chain of accountability for access to health data;
- Restrict access to information based upon the “need to know” principle;
- Establish requirements and guidelines for appropriate use and disclosure of information;
- Maintain information accuracy, consistency and integrity;

- Enable a trust relationship between *health*netBC participants; and,
- Provide a consistent framework for implementing security in the health sector.
- Be consistent with ISO17799 “Information Technology – Code of Practice for information security management”.

5 Security Policy Statement

Compliance with the following security policy statements is mandatory for all *health*netBC participants. Detailed requirements and specifications for these policies are described in the subsequent sections of this volume.

1. In the event of conflict between the requirements of the *Freedom of Information and Protection of* Privacy *Act (FOIPPA)* [1] or other legislation, and any agreements between the Ministry of Health and a *health*netBC participant and/or the requirements of this document, the requirements of legislation will be paramount. Conflicts and related issues are to be promptly referred to *health*netBC.

2. *health*netBC users and participants are required to sign a usage agreement. The Ministry of Health Services will determine the form of agreement to be used prior to establishing connections.

3. *health*netBC participants must formally delegate the responsibility and authority to approve access to *health*netBC services to selected individuals (authorizers) within the organization. Authorizers must maintain appropriate records of those approvals. Access to *health*netBC services must be provided only after the approval is granted.

4. All access to *health*netBC services must be based upon a genuine “need to know” basis directly related to the delivery or support of health services within British Columbia. Individuals are not entitled to access merely because of status, rank or office.

5. All access to or provision of personal information, as defined by the FOIPPA[1] must be supported by an audit trail which enables:
   - Identification of the individual who made the access;
   - Identification of the information accessed;
   - Determination of when the access occurred (i.e. a date/timestamp).
6. *health*netBC participants must ensure those individuals with access to *health*netBC services are aware of information privacy and security rules and practices and of

[1] See http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm

their responsibilities for appropriate access, use and disclosure of information.

6 Security Controls

To support and enable the preceding security policy statements, it is the responsibility of *health*netBC participants to establish and maintain effective security controls and procedures. Sending system controls and procedures must include the following:

6.1 Authorization

1. *health*netBC participants must identify individuals in their organizations (authorizers) who have the exclusive authority to grant, or authorize the granting, of access to sending systems that provide access to *health*netBC services.

2. *health*netBC participants must maintain up to date records of individuals who have been designated as authorizers, including an audit trail of individuals who have been designated as authorizers.

3. An authorizer must approve all access to sending systems, which provide access to *health*netBC services, and records must be kept of these authorizations.

4. Authorizers must ensure that individuals to whom they grant access have a genuine "need to know" which is directly related to their job functions or duties.

6.2 Security and Privacy Awareness Program

*health*netBC participants should implement an ongoing security and privacy awareness program for all staff. The program should review applicable policies and standards and cover user responsibilities for security and privacy.

Most Professional Colleges (e.g. College of Physicians and Surgeons of B.C. or College of Pharmacists of B.C.) have published codes of ethics for privacy and confidentiality of patient information. The Ministry of Management Services has several publications and guides which are available at: http://www.mser.gov.bc.ca/FOI_POP/. Additionally, the COACH (www.coachorg.com) publication "Guidelines for the Protection of Health Information" includes a section on educational awareness programs for the health sector.

6.3 Account Management

1. Each user accessing a sending system **must** be issued a distinct user account against which all sending activity is recorded.
2. *health*netBC participants **must** maintain records correlating individuals with user accounts. For *health*netBC audit purposes these records **must** be kept for a minimum of two years.
3. Users of sending systems – whether employees, contractors, volunteers, or others - **must** have signed a confidentiality undertaking prior to using the sending system. A sample confidentiality undertaking is available from *health*netBC.
4. The confidentiality undertaking (referenced above) **should** be supported by an organizational policy for security, confidentiality and privacy. A confidentiality undertaking could be incorporated into employee terms and conditions of employment.
5. *health*netBC participants **must** Implement procedures to ensure that sending system users are made aware of *health*netBC confidentiality and security requirements as described in this document.
6. User accounts **must** not be shared by between users.
7. Distinct user accounts **must** be issued to one and only one individual. (For Example, Dolly Smith is issued “dsmith” Dolly then retires. Later Douglas Smith joins the organization. The user ID “dsmith” may not be re-issued to Douglas Smith).
8. User accounts **must** be reviewed at least annually to confirm that all accounts are:
    a. only held by individuals who are currently employed by or associated with the participant, and
    b. continue to have a “need to know” directly related to their job function or duties
9. Records of user account reviews **must** be kept for a minimum of two years for audit purposes.
10. User accounts **must** be disabled and/or deleted in a timely manner when:
    a. a user’s employment or association with the participant ends, or
    b. a user’s job functions no longer require access to *health*netBC services
11. User accounts **should** be disabled within 2 days of departure.
12. When users are on extended leave, users accounts **should** be disabled.
13. Access to, and use of, sending system security controls (e.g. granting access rights; account definition; password management):
    a. **must** be performed with an administrator account, and
    b. **must not** be performed with an account used for accessing *health*netBC services.

6.4 Access Control

1. Security controls on sending systems **must** limit user access to only those healthnetBC services directly related to the needs of the user.
2. Participants **must** maintain records of access rights indicating user account, date and rights granted or removed.
3. Sending systems **must** have a feature that clears the screen of personal[1] and confidential information when a HealthnetBC session has been inactive for more than 15 minutes. (Two examples are locking screen savers and automatic disconnection of inactive sessions). The display **must** remain clear of personal and confidential information until an authorized user completes a re-authentication (e.g. enters a valid password).
4. Sending systems **must** identify the users initiating healthnetBC transactions, based on positive action (card swipe, password input or equivalent).
5. Computer screens and printers **must** be located so as to prevent viewing of information by the public or by unauthorized staff.

Additional access control requirements, unique to each agency's access to HealthnetBC services, are documented in the business rules in Volume 3 of this publication.

6.5 User Authentication

1. Participants **must** submit to healthnetBC a brief written description of the sending system authentication scheme. [2]
2. Users **must** successfully respond to a proof-of-identity challenge (e.g. password/shared secret, biometric comparison, proof of possession of physical token assigned to individual, proof of possession of cryptographic token assigned to individual etc.) before access to user accounts are granted.
3. Where users are connecting to the sending system over a network – such as the Internet – that would not be deemed 'trustworthy' as defined in Overview/Security Context, the proof-of-identity challenge **must** consist of **at least two** proof-of-identity mechanisms of distinctly different types (e.g. (1) shared secret, plus (2) proof-of-possession of a device).
4. The sending system **must** disable (revoke) an account or userid after 5 consecutive failed access attempts. From a security perspective, 5 consecutive failures within one minute are the same as 5 consecutive failures over a period of days or weeks. Disabled accounts or userids **must** only be re-activated by the account administrator or designate.

[1] See http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm#schedule_1

5. Where passwords or other form of shared secret are used to authenticate users, the following rules apply:
    a) Each user **must** be able to set their own password.
    b) Users **must** be instructed not to share passwords with other users or managers.
    c) The system **must** require users to set a new password after a password has been reset or a new account/userid is assigned by the account administrator.
    d) Account administrators **must** have the ability to re-set user's passwords.
    e) Passwords **must** be stored by the sending system in an encrypted file that cannot be directly read by system administrators or other users.
    f) Password characters **must not** be displayed on monitors when entered.
    g) Passwords **must not** be hard coded into any system file or routine and must be keyed in by the user each time the user signs on.
    h) Passwords **must** be at least 6 characters long.
    i) Passwords **must** be changed at least every 42 days.
    j) When a password expires the user **must** be forced to assign a new password before accessing *health*netBC business services
    k) Passwords **must** not be immediately reused.
    l) Passwords **should** include numeric and non-alpha characters.
    m) Users **must not** use the "Save Password" function of some software.

6. Where swipe cards, smart cards or other technologies (tokens) are used as the sole mechanism to authenticate users, the following rules apply:
    a) The responsibility for determining the efficacy of these systems lies with the *health*netBC participant.
    b) Each token **must** be assigned to only one user for their exclusive use.
    c) The sending system administrator **must** be able to activate and deactivate individual tokens.
    d) Users **must** keep tokens in their possession or control at all times.
    g) Un-issued cards **must** be controlled and stored in secure facilities.
    h) Procedures **must** be implemented for prompt disabling of lost cards and cards not returned by a cardholder when they no longer have a need to access the system.
7. Where a biometric authentication system is used to authenticate users, the following rules apply:

a) The responsibility for determining the efficacy of biometric systems lies with the participant organization.

b) Procedures **must** be implemented for prompt disabling of access for users when they no longer have a need to access the system.

6.6 Remote Access to Sending Systems

1. Where the sending system is not explicitly designed to be remotely accessed by end users, all remote access to sending systems (e.g. dial in access by system support technicians) **must**:

   a) Be approved by the head of the local organization.

   b) Provide access and security controls as described in this section of this document.

   c) Provide encryption of personal information (as defined by the FOIPP Act[2]) while that information is transmitted.

2. For systems that provide access to PharmaNet:

   a) Hospital emergency department systems **must not** provide remote access to PharmaNet. **Exception:** This restriction does not preclude remote access by a software vendor for the purpose of supporting sending system software.

   b) The modem should be turned off when not in use; CPBC

   c) Modems with password prompts should be used; CPBC

   d) Dialback modems should be used in order to decrease the risk of exposure to the sending system patient records. CPBC

6.7 Audit Logs

To provide transaction auditability and accountability by *health*netBC, each interaction with *health*netBC requires identification of the user initiating the transaction available on an electronic audit log.

1. The sending system **must** create an audit record, as specified in this section, for both successful and unsuccessful executions of each *health*netBC transaction.
2. The receiving system **must** create an audit record, as specified in this section, for both successful and unsuccessful executions of each *health*netBC transaction.
3. At a minimum, audit logs **must** include the following data elements for each *health*netBC transaction:

[2] See http://www.qp.gov.bc.ca/stat_req/statutes/16500.htm

Field	HL7 Element Name
Date/time of transaction	Date/Time of Message on MSH
Sending Network Facility ID	Sending Facility on MSH
Sending Application ID	Sending Application on MSH
Receiving Network Facility ID	Receiving Facility on MSH
Receiving Application ID	Receiving Application on MSH
Transaction Identification	Message Type field on MSH (=MSH.9) [3]
Unique Transaction ID	Message Control ID on MSH
Sending system user who created/sent transaction	Security on MSH

4. In large organizations (e.g. hospitals), the audit log **should** include physical location of the workstation used to initiate the transaction.
5. *health*netBC participants **must** make audit logs available to auditors and/or inspectors designated by the Ministry of Health and, in the case of accesses to PharmaNet, inspectors and/or auditors designated by the College of Pharmacists of British Columbia.
6. Audit logs **must** be retained for a minimum of two years in machine-readable form. The log(s) must be unalterable.
7. Sending system software **must** be able to produce reports from the audit logs. At a minimum, the reporting capability must provide for a report showing all accesses to *health*netBC by user, transaction and date. *health*netBC participants should establish procedures for regular review of these reports. The purpose of these reports is to provide management of the participant with a tool for monitoring for inappropriate access or use of *health*netBC services.
8. Sending system software **should** log failed attempts to access the sending system. *health*netBC participants should establish procedures for regular review of this information. The purpose for auditing access failures is to detect repeated and deliberate attempts to breach the security of the sending system.

Additional, unique audit logging requirements may apply to each agency's access to *health*netBC. These requirements, if necessary, are specified in Volume 3.

6.8 Internet Access – Outbound

1. Outbound access privileges to the Internet from the sending system **must**

   be approved by the head of the *health*netBC participant;
2. SPAN/BC reserves the right to prevent outbound access to sites considered undesirable by the Government of BC. Additionally, SPAN/BC reserves the right to

monitor usage. SPAN/BC services must only be used for accessing sites and services that are directly related to the provision of health services.

6.9 Internet Access – Inbound

1. All access privileges to the sending system from the Internet must:
    a) Be approved by the head of the *health*netBC organization;
    b) Adhere to the access and security controls detailed in this document.
2. Where the sending system is not explicitly designed to be accessed by end users over the Internet, the sending system **must** generate weekly (preferably daily) audit reports of failed accesses to facilitate follow up of attempted or potential system intrusions. The head of the local organization **must** implement a review process for the audit reports.

6.10 Encryption

1. All *health*netBC data must be encrypted when:
    a) the data is transmitted outside a 'trustworthy' network as defined in the 'Overview – Security Context' section, above;
    b) the network connections are between two or more *health*netBC participants; or,
    c) the network is shared by more than one business entity.

7 HNSECURE – New Application Development

7.1 HNSecure Business Overview

HNSecure provides secure transport for HL7 transactions and binary files attached to HL7 transactions over IP networks.

HNSecure has three main components. One component, called HNCLIENT, is used by sending system software to encrypt transactions and authenticate network end points for each transaction. The second component, called HNGATE, is a gateway/router service. The third component, called HNGARD, is the network directory server. HNGARD and HNGATE track registered HNSecure facilities, confirm that the facility on each transaction is registered and direct transactions to the appropriate receiving system.

The goal of HNSecure is to establish a secure information access infrastructure. The infrastructure supports data exchange between various *health*netBC participants, not just MoH systems. MoH is simply another participant, making its information base available to other participants. This means HL7 transactions using HNSecure can be sent to compliant computer applications at the Ministry and/or to other health related agencies.

Access to the Ministry's Client Registry can be via the transactions that were part of the original PharmaNet transaction set (i.e.: TPA, TPH, TPN) or the new transactions available through the Client Registry using HNSecure.

7.2 HNSecure Infrastructure

The HNSecure infrastructure consists of:

1. HNSecure Developers Toolkit

   The toolkit contains sample HNCLIENT programs and APIs. HNCLIENT provides sending system software with an interface routine, a network gateway, and security services including:

   a. transaction encryption and decryption to protect the transaction and its data while in transit; and,

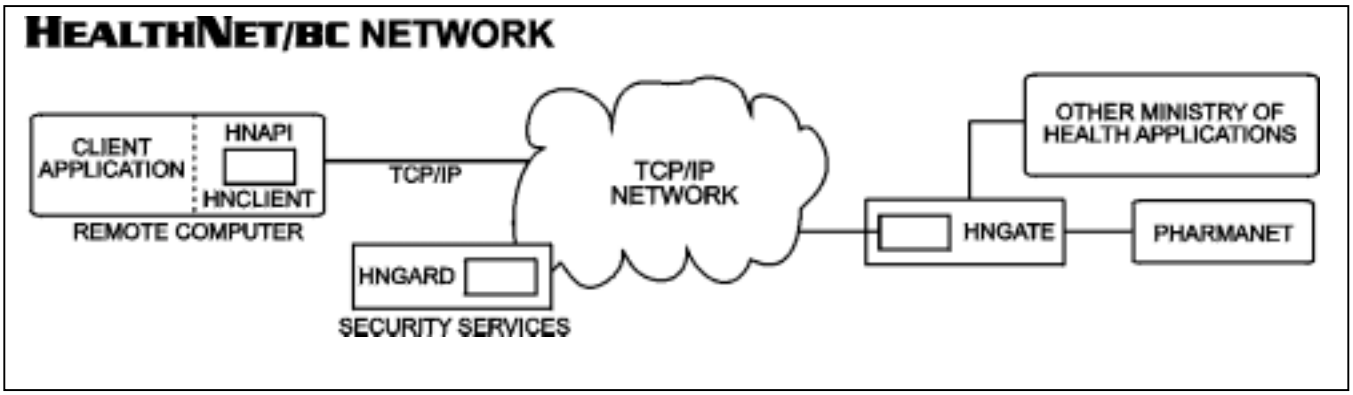
   b. authentication of network end points (i.e., client site and server site).

HNCLIENT is designed to be scalable from single PC to shared multi-user, multi-application mainframe.

2. Standards

Standards used by HNSecure are IP as the network connection protocol and HL7 as the transaction format standard, with provision to handle other data standards such as DICOM, X.12, and TIFF.

Sending system software (client applications) is developed by various SSOs and implemented in a variety of environments.



HNCLIENT is a background network gateway and security service which includes HNAPI, a software interface routine. HNCLIENT provides the sending system interface into *health*netBC. It supports all the functions required to establish secure connections to any receiving system (server applications) in the *health*netBC network. A developer's toolkit is provided by the Ministry to simplify the development of secure *health*netBC sending system software.

HNGARD is a central *health*netBC security and directory/key server which provides the services necessary to establish secure connections between sending system and receiving system applications in the *health*netBC network.

HNGATE is a gateway which provides access to receiving system applications and databases. HNGATE will be used by a variety of institutions, including the Ministry of Health, willing/able to provide secure access to clinical or health related administrative applications and databases which they manage and control.

There can be multiple HNCLIENTs and HNGATEs on the network, but only one HNGARD network directory.

7.2.1 HNCLIENT As A Gateway

HNCLIENT can be configured to act as a gateway service for one or more machines for platforms other than Windows 9x/NT. When HNCLIENT is used as a gateway other computers connect to it via remote socket calls across an IP network to send HL7 messages. HNCLIENT then encapsulates the message in the HNSecure protocol, sends it to its destination, waits for a response, decrypts the response and passes it back to the calling computer.

Using HNCLIENT as a gateway results in security exposures that are not present when HNCLIENT is used locally by each computer. Data can be transmitted, in an unencrypted format, across the Local Area Network. In addition HNCLIENT listens and responds to remote socket connections, instead of accepting only local socket connections.

As every network topology is different, it is advisable to review planned implementations with the *health*netBC team (see Section 1.4 Contacts) to ensure planned security precautions will meet the approval of MoH. MoH reserves the right to disable the use of HNSecure for any facility that is not enforcing appropriate security measures.

The following rules and guidelines apply to the management of the machine where HNCLIENT is being used as a gateway:

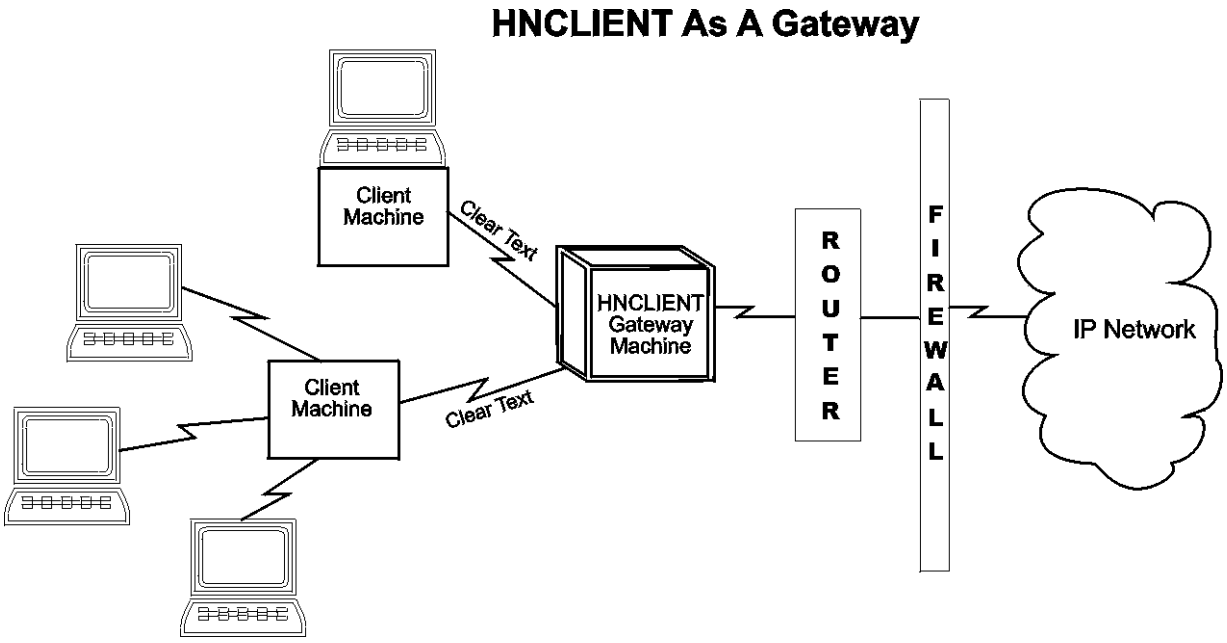
1. The *health*netBC participant must document and enforce a policy governing security practices and access to both the gateway machine and the client machines. This policy should detail what is acceptable and what is prohibited in the collection of and disposition of data collected in the course of network analysis.
2. The gateway machine must NOT have modems attached that will accept incoming calls.
3. The gateway machine must be set up to prevent unauthorized use of HNCLIENT. One way to accomplish this is to make use of HNCLIENT's IP filtering capability.
4. Log files must be kept for a minimum of two years. The log file must contain the originating IP address for all messages including connections that were rejected. See Section 6.1.4 Security Controls, for additional contents of the log file.

The HNCLIENT gateway is intended to be operated by the participant on a secure LAN. The controls on the LAN should include the following:

1. The gateway machine should not allow remote connections of any kind, other than on the single HNCLIENT socket that is listening for transactions from the client machines.

2. The host organization should have both physical and managerial control of the network segment on which the gateway machine and client machines reside.

The network segment on which the gateway and client machines reside should be secure from the unauthorized use of packet sniffing devices.



7.3 HNSecure Business Rules

7.3.1 Registration for HNSecure

All applications using HNSecure must be registered with *health*netBC. This includes applications under development as well as production applications installed at client sites.

SSOs and client site administrators must register each instance of HNCLIENT with the *health*netBC Connection Coordinator. If HNCLIENT is installed on individual machines, each HNCLIENT must be registered.

SSO Registration

SSOs use the following steps to register for and obtain a copy of the HNSecure Developers Toolkit and documentation:

1. Register for the MoH intranet web site at URL: http://admin.moh.hnet.bc.ca

2. Link to *health*netBC HNSecure information at URL: http://healthnet.hnet.bc.ca/catalogu/phase3/index.html
3. Register for HNSecure Toolkit at URL: http://healthnet.hnet.bc.ca/catalogu/phase3/index.html#register
4. Read the Ministry of Health Disclaimer.
5. Submit the completed registration form located on the web.

Once the registration is received, the *health*netBC Connections Coordinator registers the site in the HNGARD directory/key server database, and sends an e-mail confirmation to the registrant, including the *health*netBC Network Facility ID and the Registration Key.

Return to the website, and download the HNSecure Toolkit and associated documentation.

7.3.2 HNSecure Sending System Software (Client Application)

1. The HNCLIENT component of the sending system software must be able to send encrypted transactions and receive the encrypted responses properly. This includes the ability to validate the transaction digest based on the decrypted clear text HL7 transaction to prove the response transaction is valid, is returned by the targeted server, and is not corrupted in transit.
2. The sending system software must authenticate the identity of the current user. This could be done by using standard operating system logon services (UNIX, VMS, MVS, Windows/NT) or by the application itself. For applications which require a higher level of information protection and user identification, other technologies such as SmartCards with Cryptographic Authentication could be used where required. Batch programs which generate *health*netBC transactions must be designed to uniquely identify themselves. In some instances some applications may include the authenticated user identification in the MSH "security" field.
3. Logging facilities must be available to the HNSecure user. End users must be able to turn on the log and view its contents when troubleshooting with the Ministry's Help Desk or their SSO. The log file must contain at a minimum:

- Decrypted MSH from sent/received transactions;
- Signature hash values;
- Destination IP/Port; and,
- HL7 error messages.

4. Sending system software using HNSecure must display an easily-discernable indicator on all screens as to which environment is being accessed when not pointing to the production environment.

Sending system software using HNSecure must use different application level userids in production than those used in all other environments.

7.3.3 *health*netBC HNSecure - Implementation

Client Site Registration

Each instance of HNCLIENT running at a client site must be individually registered with HNGARD with a separate network facility id. No two or more instances of HNCLIENT may share the same installation and configuration information.

HNSecure Client Set-Up

After successful registration, run HNSETUP to configure HNCLIENT.

The registration number and Network Facility ID must be kept on hand if reconfiguration or reinstallation is necessary. The registration number must be kept confidential. It is suggested that it be kept in a sealed envelope in a locked drawer.

It must be possible for the sending system users to change the setup parameters, including the password and public/private key pair at any time.

The client must not provide an unauthorized *health*netBC access point such as non-fire walled Internet access or an unsecured remote access point.

HNSecure Security Features

Physical security and password management must conform to the *health*netBC Security requirements, as outlined elsewhere in Section 6 of this document. Sending system software using HNSecure must include the following security features:

1. The DES key required by the encryption algorithm must be unique for every new transaction.

2. The Network-Facility-ID assigned to HNCLIENT must be included in every transaction. HNCLIENT will insert it, if it is missing or it will validate it if it is there.

3. The sending system software must prompt the user to provide the facility password each time HNCLIENT starts up. The facility password is defined by the user when setting up HNCLIENT.

4. The facility password must not be supplied on the command line or from a publicly accessible file.

5. The facility password must not be displayed while being entered.

7.4 HNSECURE - HL7 Transaction and File Formats

HNSecure transaction formats are based on HL7 Version 2.3 and 2.4 standards with data segment (Z segment) extensions as required by individual applications. Immediate response transaction formats remain compatible with HL7 Version 2.1, 2.2, and 2.3 standards.

7.4.1 HNSecure MSH Segment

Use of the MSH segment for individual transactions is defined in Volume 4 - HL7 Message Specifications.

MSH handling by HNSecure is described in Volume 5 - Network Transmissions and Response.

7.4.2 HNSecure MSA Acknowledgment Segment

Use of the MSA segment for individual transactions is defined in Volume 4 - HL7 Message Specifications.

MSA handling by HNSecure is described in Volume 5 - Network Transmissions and Response.

7.4.3 HNSecure Binary Data Segments

HNSecure does not currently support embedded binary data in HL7 transaction segments.

7.4.4 HNSecure File Transfer Services

Note: The following service is available, however a server application is required to support the file transfer. To date there are no such server applications at the Ministry of Health.

HNSecure provides a facility for client applications to send/receive files to/from any server application which supports the file transfer protocol. File transfers are requested by specifying a message-type extension of "ZFG" (get a file) or "ZFP" (send a file) in the MSH header and providing a local file name to HNAPI/HNCLIENT. The file is attached to the HL7 message (ZFP) or response (ZFG) and read/written from/to the local file name. The MSH continuation pointer field is used to specify the logical network file name (object key) of the file. Large files should be compressed using standard compression utilities before transmission. Files are automatically encrypted to ensure consistent secure transmission of information.

While HNSecure supports the transmission of files, it is up to a file server application to manage these files. Remote clients should only be allowed to read/write files in their own private directory. For file retrieval requests, a file may also be returned from a public directory at the discretion of the files server application.

HNSecure does not provide the ability to obtain a list of available files. To obtain a specific file name for retrieval, the client application may obtain file name references from the file server application through the use of HL7 message Reference Pointers as defined by the HL7 standard.

Sample exchange protocol to obtain a file from the server:

- obtain the filename by sending an application specific HL7 inquiry message to a server application;
- the server application returns an HL7 response with Reference Pointer;
- retrieve the file from the file server application using a file transfer request (ZFG) e.g., send a PHN to the Registry, receive personal information and Reference Pointer used to retrieve the person's photo-ID.

Sample exchange protocol to send a file to the server:

- send the file to the file server application using a file transfer request (ZFP).

7.4.5 HNSecure Private Key Storage Requirements

Integrity of transaction flow between a client site and the remote server depends on protection of the private keys. Applications using HNSecure must store the private key(s) in a protected manner. One of the following

methods must be used to store configuration information which includes the private key. The data stored in the 'PrivateKey' item must be encrypted so the extraction of the true Private Key is not trivial.

All Platforms

For all platforms, the standard mechanism for configuration storage is supported. This information must be stored in a standard text file and have the following format:

FacilityID	=	BCnnnnnnnn
Domain	=	C
HNGard1IP	=	xxx.xxx.xxx.xxx
HNGard1Port	=	19410
HNGard2IP	=	xxx.xxx.xxx.xxx
HNGard2Port	=	19420
BackupHNGard1	=	hngard1.hnet.bc.ca
BackupHNGard2	=	hngard2.hnet.bc.ca
Timeout	=	70
PublicKeyLen	=	10
PublicKey	=	02 27 5f 6b 26 df 99 5a 35 b5
PrivateKeyLen	=	12
PrivateKey	=	8d 75 d8 cb 84 e0 5f 1e 99 77 0e bc
HNGardPublicKeyLen	=	6
HNGardPublicKey	=	06 44 30 e1 67 18

This file may contain other lines and configuration information but it must contain the above lines for each Network Facility ID. This file must be stored in the same directory as the executable file.

Win95/98/NT Platform

Storing the configuration information into the Windows Registry is also supported. The sub key that holds the configuration information must be the same format as described above for 'All Platforms'. The HNCLIENT sub key must be stored in the same sub key as the other keys for other applications:

HKEY_LOCAL_MACHINE

```
MINISTRY_OF_HEALTH\
HNCLIENT\
ID\
FacilityID      REG_SZ          BCnnnnnnnn
Domain REG_SZ       C
HNGard1IP       REG_SZ          xxx.xxx.xxx.xxx
HNGard1Port     REG_DWORD  19410
HNGard2IP       REG_SZ          xxx.xxx.xxx.xxx
HNGard2Port     REG_DWORD  19420
BackupHNGard1       REG_SZ          hngard1.hnet.bc.ca
BackupHNGard2       REG_SZ          hngard2.hnet.bc.ca
Timeout         REG_DWORD  70
PublicKeyLen    REG_DWORD  10
PublicKey       REG_BINARY   02 27 5f 6b 26 df 99 5a 35 b5
PrivateKeyLen   REG_DWORD  12
PrivateKey      REG_BINARY   8d 75 d8 cb 84 e0 5f 1e 99 77 0e bc
HNGardPublicKeyLen  REG_DWORD  6
HNGardPublicKey     REG_BINARY   06 44 30 e1 67 18
```

Document History

DOCUMENT MODIFICATION HISTORY		
Version	Release Date	Description
2.0	September 1999	Original publication
3.0	November 21, 2003	Former HRS Chapter 6 re-published as separate volume. Security policies and procedures updated. V2.0 reference to HNSecure File Transfer service removed. This service was not implemented.

[1] 02/Nov/27 – example of correction
[2] New requirement.
[3] Clarification. The log should capture the two components of MSH.9. The first component is named the same as the field; that is, 'Message Type'. The second component is 'Trigger Event' code. On older *healthnetBC* messages the second component was not valued. However, recent messages now include this HL7-required component. If present, it should be captured in the log along with message type.