



# **Accessing the Ministry Web Business Services**

---

## ***Access Administrator's Guide***

Prepared by *healthnetBC* Access Services (HAS)  
*healthnetBC*  
IST, Knowledge Management & Technology

Version 3.1

April 2004

# Contents

## Contents i

<b>1. About this Guide.....</b>	<b>3</b>
Purpose & Audience.....	3
<b>2. Introduction.....</b>	<b>3</b>
<b>3. Access Administrator Appointment.....</b>	<b>3</b>
<b>4. Access Administrator Responsibilities.....</b>	<b>4</b>
User Administration.....	4
Digital Certificate Administration.....	4
Communication.....	4
Support.....	5
<b>5. Help Desk Support .....</b>	<b>5</b>
Ministry of Health Services HelpDesk.....	5
healthnetBC HelpDesk.....	5
<b>6. Security 6</b>	
Access.....	6
About Digital Certificates.....	6
<b>6. System Requirements .....</b>	<b>6</b>
Web Browser.....	6
<b>7. Connection Activities .....</b>	<b>7</b>
Confirmation of Approved Web Business Services.....	7
Determine User Access.....	7
Determine Service Permission Group.....	7
Collect Confidentiality Undertaking.....	8
Register Users.....	9

Receive Confirmation E-mail .....	9
Install Digital Certificate .....	9
Provide Instructions to User .....	10

## **9. Other Administrative Functions ..... 10**

Cancel Access Permission .....	10
Request Additional Business Services .....	11
Change MSP Group Plan Administration .....	11
Change Access Administrators .....	11

# 1. About this Guide

---

## Purpose & Audience

This document provides information and procedures for the *Access Administrator* assigned to your organization. The *Access Administrator* is responsible for coordinating all user access to *healthnetBC* Web Business Services.

# 2. Introduction

*healthnetBC* Web Business Services provides convenient Web access to information through Ministry systems and services. This information is used in a variety of ways, from determining whether a specific client is eligible for health services, to helping an employer administer employee's Medical Service Plan premiums.

Because of the private nature of the client data, worldwide access via Web to that data, and the potential for fraud, the system must be certain of user identity and authorization. *healthnetBC* Web Business Services uses two security mechanisms:

1. UserIDs and passwords to identify users; and
2. Digital certificates to ensure that the user is access the business services through a valid computer, in a trusted organization.

# 3. Access Administrator Appointment

The organization's CEO, or designated Signing Authority, is required to appoint an *Access Administrator*(s) as the primary contact between your organization and the Ministry of Health Services, who will manage all user access to Ministry systems and services. The *Access Administrator* is the only individual within your organization authorized to register users.

*Access Administrator* appointments can be sent via e-mail to [HLTH.HnetConnection@gems1.gov.bc.ca](mailto:HLTH.HnetConnection@gems1.gov.bc.ca), or by fax to “Attention: *healthnetBC* Access Services” at (250) 952- 1119.

## 4. Access Administrator Responsibilities

*Access administrators* are responsible for ensuring secure access within the organization, user registration, assigning permissions to users, and coordinating the installation of the Ministry issued digital certificates onto users computers.

Access Administrator duties include:

---

### User Administration

- registering users;
- assigning and cancelling access permissions;
- maintaining current user access records;
- reviewing user access permissions on a regular basis;
- conveying the importance of security requirements, confidentiality of information and protection of UserIDs and passwords to all authorized users. UserIDs and passwords **MUST NOT** be shared.
- maintaining security requirements;
- ensuring secure storage of signed confidentiality undertakings.

---

### Digital Certificate Administration

- coordinating the installation of the Ministry's digital certificate on the computers of authorized users;
- removing digital certificates when a computer is no longer used to access *healthnetBC* Web Business Services ;
- ensuring secure storage of the digital certificate(s).

---

### Communication

- receiving and distributing Ministry communications related to user access and system issues.

---

## Support

- acting as the first point of contact for users when they have a problem accessing the system. Unresolved problems can be referred to the *healthnetBC* Help Desk.

# 5. Help Desk Support

---

## Ministry of Health Services HelpDesk

Ministry of Health Services HelpDesk is available Monday to Friday, 8:00 a.m. - 4:30 p.m. PST to accept calls and provide the digital certificate password for your organization.

**The Ministry of Health Services HelpDesk is available at (250) 952-1234.**

---

## *healthnetBC* HelpDesk

***healthnetBC* HelpDesk** is available 24 hours per day, 7 days a week, to accept, log and resolve problems experienced by users accessing the *healthnetBC* services. The level of support may be limited outside of regular business hours.

<b><i>healthnetBC</i> HelpDesk</b>	<b>Phone Numbers</b>
<b>Vancouver and Lower Mainland</b>	<b>(604) 682-2316</b>
<b>Victoria</b>	<b>(250) 952-2293</b>
<b>Toll Free (in BC only)</b>	<b>1- (888) 764-2323</b>

## 6. Security

---

### Access

As part of the terms and conditions of the Data Access Agreement between your organization and the Ministry, your organization will be given a **Digital Certificate**. Your organization will install the certificate on all computers used to access specific Ministry Web Services, such as the *healthnetBC* Web Business Services. This certificate identifies and confirms that an authorized computer from your organization is communicating with the Ministry's Web servers.

---

### About Digital Certificates

Digital certificates are *non-forgable* electronic files used by Web browsers for identification purposes. Digital certificates work with a secret number called a *private key*. The computer uses the private key to scramble (encrypt) data. Digital certificates contain the information needed to unscramble (decrypt) the data that is scrambled by the private key.

Your private key is your organization's electronic proof of identity for the Ministry Web service(s). Protect your organization's digital certificate from theft or loss, to prevent possible fraudulent activity in your organization's name.

## 6. System Requirements

---

### Web Browser

Your computer must be running a Web browser with a cipher strength of 128-bit.

**Note: Internet Explorer (version 6.0, or higher) is the recommended Ministry standard browser**, for web-based services.

At a minimum, these Web browsers will enable access to *healthnetBC* Web Business Services:

- Netscape Navigator Version 4.04 (or higher) with 128 bit encryption; **or**
- Internet Explorer Version 5.5 (or higher) with 128 bit encryption.

## 7. Connection Activities

---

### Confirmation of Approved Web Business Services

After the Ministry has received the signed Data Access Agreement, from your CEO or designated signing authority, the appointed Access Administrator will receive a "**Confirmation of Approved Web Business Services**" e-mail from *healthnetBC* Access Services (HAS), confirming:

- your organization's unique Organization ID (ORG ID) number;
- the Service Permission Groups (SPGs) approved for use by your organization;
- approved MSP Group Account Numbers, if applicable (for MSP Coverage Maintenance services only);
- instructions for completing the remaining connection process; and
- your organization's digital certificate (approximately 3Kb).

#### **To Save the Digital Certificate from the e-mail to a diskette:**

1. Double-click on the attachment file within the e-mail
2. On the **Opening Mail Attachment** dialog box, select **Save it to disk**
3. Insert a diskette in the machine's floppy drive, and **Save** the file to that drive.

This diskette will be required to install the digital certificate to each machine where users require access to the *healthnetBC* Web Business Services.

#### **Security Note:**

This diskette should be retained in a secured location.

---

### Determine User Access

The *Access Administrator* will determine:

- which staff members require access to the *healthnetBC* Web Business Services;
- which business services each user requires to perform their job; and
- the appropriate Service Permission Group (SPG) for each user.

---

### Determine Service Permission Group

*healthnetBC* Web Business Services are offered in packages called *Service Permission Groups (SPGs)*, which consist of one or more services. An organization can have permission to use more than one SPG, however each user can only be assigned to one SPG at one time. The assigned SPG restricts the user to only the transactions and data

required to do their work. The business services available to an organization are defined when the organization signs up to use *healthnetBC* Web Business Services.

As new business services are developed and new types of clients are authorized for access, many *Service Permission Groups* will be developed.

Some of the existing *Service Permission Groups (SPGs)* are listed below, for reference:

**Hospital Admitting** - assigned to users responsible for confirming patient eligibility for publicly funded health care, assigning PHNs and updating patient demographics. Typically, this SPG is used for Admitting and Finance functions within a hospital.

**Continuing Care Client Search** - assigned to users responsible for Continuing Care clients. These services are a subset of the **Hospital Admitting** SPG and are used to confirm eligibility for publicly funded health care services and person demographics.

**Mental Health Client Search** - assigned to users responsible for Mental Health clients. These services are a subset of the **Hospital Admitting** SPG and are used to confirm patient eligibility for publicly funded Health Care services, confirm person demographics, and assign a PHN to a client if they do not have one.

**MSP Coverage Maintenance** – assigned to users responsible for MSP premium administration for employees. Typically, this SPG is used for Payroll or Employee Benefits functions.

**Primary Health Care** - assigned to users within designated Primary Health Care Sites. These services are a subset of the **Hospital Admitting** SPG and are used to confirm eligibility for publicly funded health care services and person demographics, and will allow Primary Health Care organizations/sites to manage their population-based funding patient registers.

---

## Collect Confidentiality Undertaking

Before being allowed access to *healthnetBC* Web Business Services, each user must sign a confidentiality pledge or undertaking, in which they promise to treat as confidential all Ministry client information to which they have access. *Access Administrators* must ensure that these undertakings are signed before granting access to services.

Signed confidentiality undertakings are to be retained by the organization and used in conjunction with an education program related to privacy and confidentiality of client records.

**The organization must produce the signed confidentiality undertaking for review and audit, at the request of the Ministry of Health Services.**

Users within the **public sector** (hospital employees, etc.) are covered by the *Freedom of Information and Protection of Privacy (FOI/POP) Act*, and as such are assumed already to have signed an appropriate confidentiality undertaking, as a requirement of their employment.

Every **private sector** user of *healthnetBC* Web Business Services must sign a pledge or undertaking which binds them to the confidential treatment of all information related to Ministry clients. The Ministry provides private sector organizations with required wording that may be used as a stand-alone undertaking or added to the organization's own confidentiality pledge.

All users in the private sector must sign Confidentiality Undertakings that meet the Ministry's requirements.

A sample copy of a Confidentiality Undertaking document is available on the *healthnetBC* Web site at [http://healthnet.hnet.bc.ca/catalogu/healthreg/confidentiality\\_undertaking.pdf](http://healthnet.hnet.bc.ca/catalogu/healthreg/confidentiality_undertaking.pdf) , as well as attached to the "*Confirmation of Approved Web Business Services*" e-mail.

---

## Register Users

The *Access Administrator* sends an e-mail request entitled "User Registration Request" to *healthnetBC* Access Services at [Hlth.hnetconnection@gems1.gov.bc.ca](mailto:Hlth.hnetconnection@gems1.gov.bc.ca) .

The following information is required for each user:

- User's Full Name;
- User's E-mail address;
- User's Telephone number and Fax number, if available;
- the name of the site location where the user will be working from;
- the Organization ID # assigned to that particular site if known ; and
- the Service Permission Group authorized for the user.

---

## Receive Confirmation E-mail

Once your registration request has been processed, you will receive an e-mail from *healthnetBC* Access Services confirming the userid and temporary password for each user.

---

## Install Digital Certificate

Each registered user must have the Ministry's digital certificate installed on his or her machine in order to access *healthnetBC* Web Business Services.

**IMPORTANT NOTE: Each user must be logged onto his/her machine, at the time the certificate is installed on that machine.**

The installation steps for the certificate depend on the browser you are using in your organization. The instructions are described in the document for your organization's specific browser:

Refer to the documents below, on the *healthnetBC* Web site:

**Client Eligibility for Health Care Services and Client Demographic Information;**

<http://healthnet.hnet.bc.ca/catalogu/healthreg/phnassign.html>

Or,

**MSP Coverage Maintenance for Group Plan Administrators;**

<http://healthnet.hnet.bc.ca/catalogu/healthreg/mspcover.html>

---

## Provide Instructions to User

As soon as the digital certificate has been successfully installed on the user's computer the *Access Administrator* can provide the user with:

- their UserID and initial Password;
- a copy of the "A Guide for New Users – Logging in to Secure Ministry Web Sites", at [http://healthnet.hnet.bc.ca/catalogu/healthreg/guide\\_for\\_new\\_users.pdf](http://healthnet.hnet.bc.ca/catalogu/healthreg/guide_for_new_users.pdf)  
This document contains login and password change instructions, HelpDesk phone numbers, etc.;
- information on available training options.

Users can then start accessing the *healthnetBC* Web Business Services.

# 9. Other Administrative Functions

---

## Cancel Access Permission

It is the *Access Administrator's* responsibility to track users of *healthnetBC* Web Business Services and be aware when users no longer require access to the services (i.e., when users change jobs, change duties, or leave the organization).

To minimize the risk of unauthorized access, it is critical that users have their access permission cancelled as soon as it is no longer required.

To cancel user access to *healthnetBC* Web Business Services send an e-mail to [Hlth.hnetconnection@gems1.gov.bc.ca](mailto:Hlth.hnetconnection@gems1.gov.bc.ca) , providing your name, e-mail address, Organization ID, and the name and UserID of the individual(s) whose access is to be cancelled.

---

## Request Additional Business Services

Your organization's business services are defined during the sign-up process. However, you may discover that your organization needs access to business services not included in your original SPG(s). To request additional business services, contact the *healthnetBC* Access Services at [HLTH.HnetConnection@gems1.gov.bc.ca](mailto:HLTH.HnetConnection@gems1.gov.bc.ca).

---

## Change MSP Group Plan Administration

To add or remove MSP Group Plan Account numbers to your organization's MSP Coverage Maintenance service send an e-mail to [HLTH.HnetConnection@gems1.gov.bc.ca](mailto:HLTH.HnetConnection@gems1.gov.bc.ca) .

---

## Change Access Administrators

If the *Access Administrator* changes (due to staffing changes, etc.), the CEO or designated signing authority must submit an e-mail to [HLTH.HnetConnection@gems1.gov.bc.ca](mailto:HLTH.HnetConnection@gems1.gov.bc.ca), naming the new *Access Administrator* whom they are appointing, along with that person's information (e-mail address, phone number, etc.).

