BRITISH COLUMBIA
Ministry of Health

HEABC
Health Employers Association of BC

HNFile for HSCIS Guide

Author:	*Managed Services Documentation Team*
Creation Date:	August 13, 2002
Last Updated:	October 14, 2020
Document Number:	
Version:	6.0

Change Record

Date	Author	Version	Change Reference
2002-07-17	Managed Services Documentation Team	3.0	Amalgamation and restructuring of manual and appendices. (**Original document: Access Administrators Guide)**
2002-08-13	Christine Monford Steve Gillman	4.0	Revised original document to produce HSCIS specific version. Added HSCIS final chapter.
2002-08-28	Christine Monford	4.1	Revised original document to update support during implementation.
2002-09-20	Christine Monford	4.2	Changed support contacts and changed diskette to email for digital certificate installation.
2002-11-01	Christine Monford	4.3	Made change to Netscape support by the Ministry.
2003-10-28	Don Tolson	4.4	Removed Ceridian and ADP as supported vendors.
2004-03-02 2004-11-25 2005-10-25	John Bidner Todd Riddell Nancy Passfield	4.5 4.6 4.6	Removed references to Ministry of Health Planning Added screen shots. Added screen shots.
2008-07-21 2010-02-04	Nancy Passfield Nancy Passfield	4.7 4.8	Added screen shots Changed Help Desk Phone Number
2012-09-30	Nancy Passfield	4.9	Updated Screen Snap shots, updated Internet Explorer from 6.0 to 7, and took out references to Netscape Navigator
2014-10-02	Caleen Taylor	5.0	Replaced references to call the Help Desk with “e-mail HLTH.HscisSupport@gov.bc.ca with your Corporate Employer Number and Legal Name in the subject line (i.e. Corp #1234 Smith Ltd.) and details in the body of the message.”
2020-10-14	Kenneth Cable	6.0	Revised original document to reflect significant changes to the website and HNFile submission process as a result of the HSCIS 3.0.1 release on October 7, 2020.

Preface

Purpose

This document provides information and procedures for coordination and system administrative support to users for the HealthNet/BC Web Services.

Audience

This document is intended primarily for users requiring access to HNFile for HSCIS (Health Sector Compensation Information System).

Structure

This document includes the following chapters.

Introduction	Introduces the document
Prerequisites	Identifies computer requirements for accessing HealthNet/BC
Registering users	Describes the tasks involved with registering users to HealthNet/BC

Terms and conventions

This document uses standard conventions for displaying information.

COURIER	Indicates text that you type.
ARIAL BOLD	Indicates a label that appears on a screen (for example, a field name or push-button label).
Italics	Indicates variable text that you type when entering a command or a citation to another document.
Bold	Use this style for emphasis.
	Indicates a note to give you additional information or to emphasize a particular procedure.
	Indicates a warning or alert. To avoid making an error, you need to pay particular attention to the information contained in these alerts.
	Indicates a useful tip or shortcut, which you can use to save time and keystrokes.

Contents

Introduction

HealthNet/BC Web Business Services provides convenient web access to basic information about Ministry clients. 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, world wide access via web to that data, and the potential for fraud, the system must be certain of user identity and authorization. HealthNet/BC Web Business Services uses two security mechanisms, user IDs and passwords to identify users and digital certificates to ensure that the user is sitting at a valid computer in a trusted organization.

Access administrators are responsible for ensuring secure access within the organization, user registration, assigning permissions to users and providing digital certificates to clients. Within the Health Authorities, access administrators have been designated but for other HSCIS submitters, HealthNet/BC Access Services provides this role.

Each user is responsible for ensuring the security of their own passwords.

Understanding secure access

The Internet is an untrustworthy network. To protect confidentiality of information sent over the Internet, and to guard against unauthorized access, HealthNet/BC Web Business Services use SSL encryption and digital certificates. Local PCs must be set up to accept these high-level security techniques.

Encryption is translating data into an unreadable form. It is the most effective way to achieve data confidentiality. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plaintext; encrypted data is called ciphertext. The encrypted data travels over the Internet using the Secure Sockets Layer protocol (SSL).

There are two kinds of encryption. One kind is based on two parties sharing knowledge of a single secret key. The secret key is used both to encrypt and decrypt the data. A problem with secret key encryption is that it is difficult to securely share the secret key between two remote parties.

The other kind of encryption is based on two mathematically related keys; one called the public Key, and the other called the 'private key'. This second kind of encryption is called Public Key encryption.

Public/private key pairs

In Public Key encryption, only the private key can decrypt information encrypted by the Public key, and vice versa. The Public and private keys are related but it is virtually impossible to figure out the private key from the public key. With this mechanism, two parties can safely pass their Public keys to each other over untrusted channels; it is not necessary to protect the Public keys. Then the respective Public keys are used to encrypt private information to be shared between them.

Anyone can know the sender's Public key used to encrypt the message. Only the recipient of the message knows the private key used to decrypt the message. Each party can be comfortable in the knowledge that only the holder of the (closely guarded) private key can decrypt the information.

The recipient's public key travels over the Internet to the sender enclosed in a digital certificate.

Digital certificates

A digital certificate is a tamper-proof document that contains a public key and some information relating to the identity of the legitimate holder of the related private key. A digital certificate can be used to verify that a user sending a message is who they claim to be and to provide the receiver with the means to encode a reply. The sender's public key and identification is included and encrypted within in the CA's certificate. With the sender's information, the recipient can read the encrypted information and return an encrypted reply.

An organization that issues digital certificates is called a Certificate Authority (CA). For HealthNet/BC Web Business Services, certificates are issued by a Government-operated CA. These certificates are for use with HealthNet/BC services only; they intentionally cannot be used by any other organizations.

SSL protocol

The Secure Sockets Layer protocol is the most widely accepted Internet authentication and encryption protocol used to set up communication between clients and servers. SSL client software use standard techniques of public key cryptography to check that a server's certificate and public key ID are valid and have been issued by a CA listed in the client's list of trusted CAs. The same is true when a server validates a client's digital certificate.

The SSL protocol includes the SSL record protocol and the SSL handshake protocol. The Record protocol defines the format used to translate the data, and the Handshake protocol involves exchanging a series of messages between server and client to establish connection.

SSL encryption comes in two strengths, 40-bit encryption and 128-bit encryption. The bit size is the length of the cryptographic code within the key. The longer the key, the more difficult it is to break the encryption code. Microsoft offer browsers that enable different levels of encryption. HealthNet/BC servers and clients require the stronger 128-bit encryption.

Directory of users

We all use directories of one sort or another every time we use the Internet or our own Intranets. The Directory Access Protocol (DAP) is the Internet standard for accessing information in the directory on the Web. LDAP is the Lightweight version for corporations or companies. You can put just about anything into directories including text, photos, URL's, pointers to whatever, binary data or Public key certificates.

The Ministry's LDAP directory authenticates their access clients in conjunction with the SSL Handshake protocol. The directory contains information about the client's server, Public key, certificates serial numbers, and validity periods. When the client is authenticated, the SSL Handshake proceeds and the client is authorized to access the requested resources.

If the certificate has been revoked from the user's entry in the LDAP directory, the server will refuse to authenticate that certificate or establish a connection.

The Access Administrator can add, modify or delete (revoke) users from the LDAP on the HealthNet/BC Web Business Services **Access Administrator's** web page. The Access Administrator function for HSCIS employers is performed by HealthNet /BC Access Services (HAS) who set up the user's userid, password, service permission group and HNFTP account in LDAP. HAS also distributes digital certificates and the associated passwords to authorized HSCIS employers.

Prerequisites

Organizations must apply to and be authorized by the Ministry to access the HealthNet/BC Web Business Services requires a jointly signed Ministry Data Access Agreement.

Checking your web browser

One of the following web browsers is required to access the HealthNet/BC Web Business Services:

- Internet Explorer Version 11 **(Supported by the Ministry**)

To determine if you are using Internet Explorer 11, do the following.

In Internet Explorer:

1. Start Internet Explorer browser.
2. On the toolbar click on the gear symbol for **Tools (Alt + x)** and select **About Internet Explorer** from the drop-down menu.

3. On the pop-up window the version number is the first line under the logo.

   If your version is less than required you will require an update from Microsoft.

4. Click **OK** to return to your browser.
5. Enter the following URL address in your browser address bar and hit **ENTER**.
   https://www.microsoft.com/en-us/download/details.aspx?id=41628
6. Follow the instructions on the screen and download Internet Explorer 11.

Ministry password requirements

The Ministry system prompts the user to change the password at the first log in and requires the password to be changed, upon expiry, every 42 days.

The password format must be:

- a minimum of six (6) characters long
- contain at least one number
- not be obviously related to the user's name or User ID

Password reuse is not allowed.

Confidentiality pledge

Before being allowed access to HealthNet/BC Web Business Services, each user must sign a confidentiality pledge or undertaking, in which they promise to treat as confidential all Ministry client information they will have access to. The Access Administrator must confirm this prior to granting user access.

Users within the **public sector** (hospital employees, etc.) are covered by the *Freedom of Information and Protection of Privacy (FOIPP) 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 HealthNet/BC 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. Access administrators must ensure that these agreements are signed before granting access to services.

Support

Contact information:

HNFile for HSCIS	E-mail Ministry of Health HSCIS Support at **HLTH.HscisSupport@gov.bc.ca** with your Corporate Employer Number and Legal Name in the subject line (i.e. Corp #1234 Smith Ltd.) and details in the body of the message.

Regular maintenance

The administrator keeps the access records current, deletes inactive users, reviews permissions, updates and removes digital certificates, and ensures secure storage of signed confidentiality forms.

Your organization's business services are defined during the sign-up process. You need to keep your organization access to business services current. Please advise the Ministry of any changes in staff by contacting the HealthNet/BC Systems Support Coordinator at HLTH.HnetConnection@gov.bc.ca .

Installing digital certificates

Each registered user must have the Ministry's digital certificate installed on his or her machine in order to access HealthNet/BC Web Business Services. At the Health Authorities, the Access Administrator is responsible for coordinating the installation of the digital certificate. For all other health employers, it is the responsibility of the person receiving the digital certificate to install on the PC which will be transmitting the data and for storing the certificate in a secure place.

HealthNet/BC Services generates the digital certificate (and creates a password), records the information in their database and then emails the certificate to the authorized user.

HealthNet/BC Services supports:

- **Internet Explorer Version 11**

If you are using a more recent version the screens presented may not be the same. Refer to the Help provided with your version of the browser in order to complete any activities described in this document.

You must log on to your machine at the time the certificate is installed.

Prior to Installing the Digital Certificate

You will receive the digital certificate as an attachment via email from the HealthNet/BC Services coordinator and must first save the file to a secure location on your personal computer or local area network (LAN). Please note the location where you have saved the digital certificate as you will need it to proceed further.

You must also contact the HealthNet/BC Services coordinator to receive the password for your digital certificate.

In Internet Explorer

If your browser is Microsoft Internet Explorer, read and follow these instructions.

1. Open your **Internet Explorer** browser
2. From the **Tools** menu from the top function bar, choose **Internet Options**.
3. Select the **Content** tab and click the **Certificates** button.

   The list box displays certificates that have been imported.
4. Click the **Import...** button.

   The **Certificate Manager Import Wizard** is displayed.
5. On the first window, click **Next**.

   The wizard displays the **Select File to Import** screen.
6. Make sure that you have copied the digital certificate from your email attachment to your PC or LAN drive.

   Select the file location with the **Browse** button.

In the **Files of Type** field, leave as "Personal Information Exchange .pfx"

7. Scroll through and locate the correct certificate file for HealthNet/BC.
8. Click the **Open** button.

   The wizard returns to the **Select File to Import** screen. The certificate file name from the diskette displays in the text box.

9. Click **Next**.

   The wizard displays the **Password Protection For Private Keys** screen.

10. Enter the password that was provided to you by the HealthNet/BC Systems Support Coordinator. You must phone them to obtain this information.
11. Select the **Enable strong private key protection** check box.

    DO NOT select *Mark The Private Key As Exportable*.

12. Click **Next**.

    The wizard displays the **Select Certificate Store** screen. Check to be sure the radio button next to **Automatically select the certificate store based on the type of certificate** is selected.

13. Click **Next**.

    The wizard displays the **Completing the Certificate Manager Import Wizard** screen.

14. Click **Finish**.

    The import program opens to the **Private Key Container** window.

15. Click the **Set Security Level...** button and set the security level to **Low**. If Low is unavailable, select Medium.
16. Click on **Next**. You are notified that you have selected Low. Click on **Finish**.
17. The import program returns to the Private Key Container screen. Click **OK**.
18. The import is successful. Click **OK**.
19. You are now returned to the Certificates window in your browser. Your certificate should be displayed in the list box. Click **Close** and **OK** to return to your browser.

Deleting a certificate from Internet Explorer

1. Open your **Internet Explorer** browser
2. From the **Tools** menu from the top function bar, choose **Internet Options**.
3. Select the **Content** tab and click the **Certificates** button.

   The list box displays certificates that have been imported.

4. On the **Personal** tab, select the certificate to be deleted. Click **Remove** .
5. On the **Certificate Manager** dialog box, click **Yes**
6. Click **Close** to return to your browser.

Final Instructions to User

As soon as the *Access Administrator* (the HealthNet/BC Systems Support Co-ordinator) activates the user they will provide each user with:

- their user ID and initial password
- the URL for the HNFile for HSCIS web site

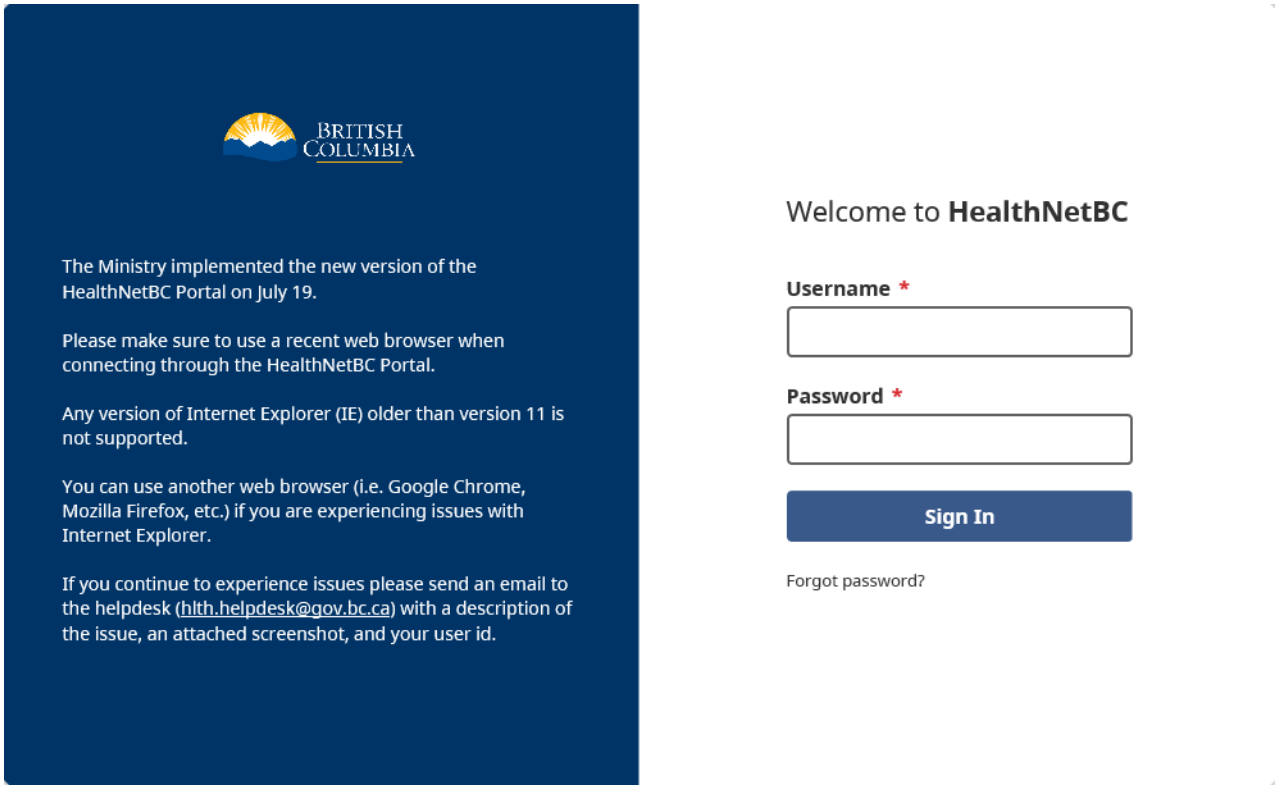
At this point users can access the HNFile for HSCIS. Please the section on Support Page 9 for how to get help.

User Guide for HSCIS HNFile

HNFile for HSCIS was designed to provide a secure and simple method for submitting payroll extract data to the HSCIS system. The new web interface, provided free by the Ministry of Health Services to HSCIS employers, replaces 'DOS' style commands for PGP encryption and HNFTP file transfer. Greater security measures are now in place with the use of a secure web site and client digital certificates.

Accessing the Web Page

The URL for the web site is https://healthnetbc.hlth.gov.bc.ca/



1. The first time you access this site, we suggest that you add it as a bookmark to your list of favourite sites for easy access the next time that you log on.
2. When you attempt to access the site, you will be prompted to select a digital certificate to use when connecting. Select the HSCIS certificate (which may be the only one you have) and click '**OK**'.
3. When presented with the Security Alert screen, click on '**Yes**'.

4. At the login screen, type in your Username, Password (that you were provided with from the Ministry) and click on '**Sign In**'.
5. The first time you access this site, you will be prompted to change your password. (see the Change Password section later in this chapter for more details.)

(**Note**: If you use HNFile for more than one application (e.g. HSCIS and CPIM), you will be given a choice of the application you want to use – click on 'HSCIS'.)

The HSCIS Home Page

The tabs and buttons on the Home Page the screen identify the options that are available to you.

The following options are available:

- **Home** – takes you to the Home page
- **Services** – takes you to the 'Services' screen
- **Change Password** – takes you to the 'Change Password' screen
- **Help** – takes you to the 'Help' screen
- **Contact Us** – takes you to the 'Contact Us' screen
- **Sign Out** – will close the session and sign off from the application
- **HSCIS** – takes you to the 'HSCIS' screen to submit payroll extract reports (HNFile)

- **HSCIS Web Service (Data Entry)** – takes you to the HSCIS Web Application

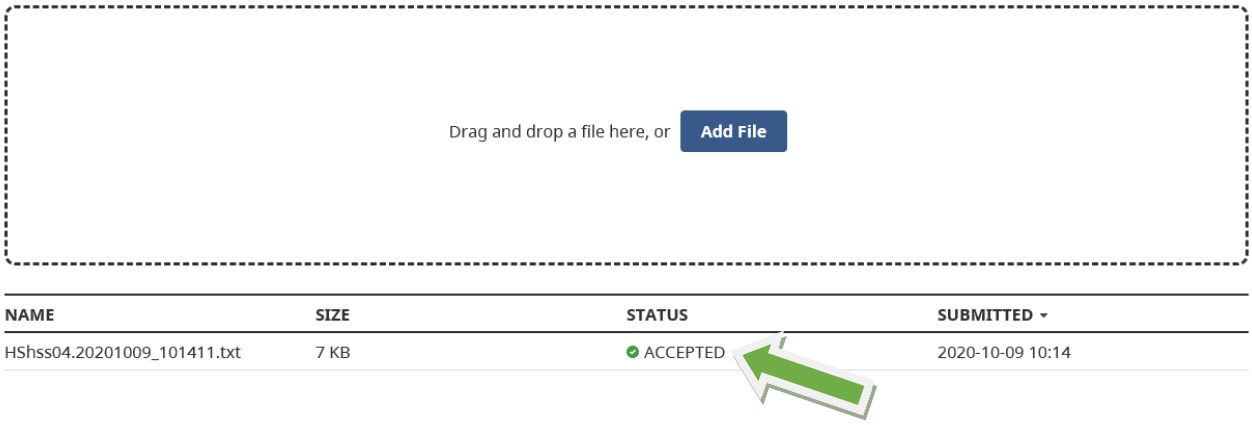
HSCIS

The **HSCIS** screen is used to submit payroll extracts to the HSCIS application for validation. To proceed click on '**Payroll**' at the top left corner of the screen.

Using the Submit Payroll Extract Screen

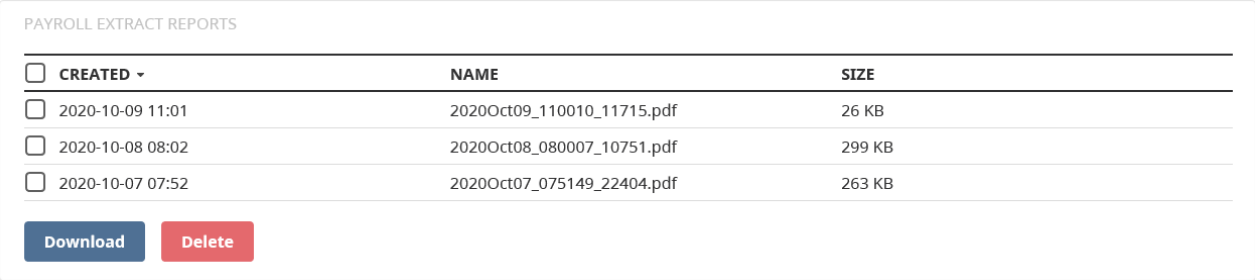
Before selecting your file to submit, please use the drop down boxes to select the appropriate account, year and quarter of the extract. HSCIS will only accept payroll extracts that are a flat text ascii file (**.txt**). Please change the file type to .txt or contact your payroll provider to have them supply a .txt extract file.

1. In the Add File area directly beneath the 'Quarter' drop down menu, drag and drop a file, or click "**Add File**' to select the file. It is recommended that you use consistent file names with a unique descriptor to help you differentiate files for validation purposes. The file must be in an accessible directory (i.e., either on your local network or on the hard drive of the PC you are using).
2. If the file was submitted properly, the file will appear in the table directly below the Add File area with a Status of "ACCEPTED".



3. After the report file has been accepted, a Validation Report will be available for download in the "Payroll Extract Reports" section at the bottom of the web page. Validation Reports are generated once per hour on week days from 8:00 am to 4:00 pm PST. Please check back later to see the report when it becomes available. If you have not received your Validation Report within 2 business days of having submitted a file, please e-mail Ministry of Health HSCIS Support at **HLTH.HscisSupport@gov.bc.ca** with your Corporate Employer Number and Legal Name in the subject line (i.e. Corp #1234 Smith Ltd.) and details in the body of the message.

Using the HSCIS – Payroll Extract Reports table



After adding a file, a list of Validation Report files will be displayed in the table for downloading. There may be more than one file for a day (e.g., if two files were submitted in one day, there will be two validation reports produced during the hourly processing). HNFile automatically date and time stamps the uploaded files and Validation reports to differentiate them.

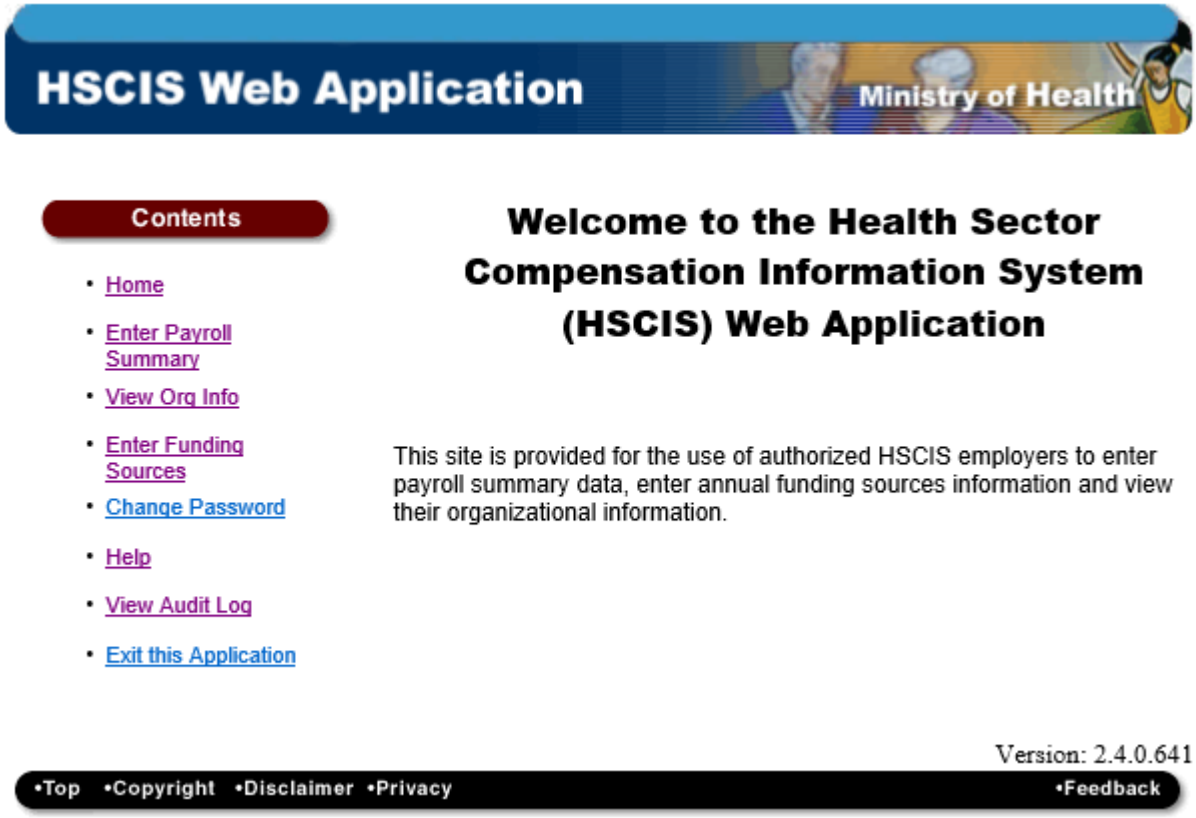
1. To access the Validation Report, check the box next to the file name, and then click the "Download" button. You can check the box next to "Created" in the header and then click the "Download" button to download all reports available. You will be asked if you want to open the file or download it to a directory on your PC or local network.
2. If you chose to open the file, it will be displayed using Adobe Acrobat reader (which must be installed on your PC).
3. To delete a file (or files), click on the check box next to the file (or files) you want to delete. To deselect a file, click again on the check box. To deselect all files, click on the box next to "Created" until all boxes are unchecked. When you are satisfied with your selection of files to delete, click on the '**Delete**' button.
4. Please read the Validation Report to see if there are any errors preventing the successful submission of the HSCIS report. If there are no errors preventing submission, then you have successfully submitted the HSCIS report.
5. If there are errors preventing successful submission, please read them carefully and make the necessary changes to the report to fix the errors, and then resubmit.

6. If the Validation Report indicates a problem that you are not able to resolve, please e-mail Ministry of Health HSCIS Support at **HLTH.HscisSupport@gov.bc.ca** with your Corporate Employer Number and Legal Name in the subject line (i.e. Corp #1234 Smith Ltd.), and attached copy of the Validation Report and error details in the body of the message.

Please Note: As an added security measure, these files will be available via the Web for 3 weeks only – please ensure that you retrieve the validation reports on a regular basis.

HSCIS Web Service (Data Entry)

To view this service, click on the 'HSCIS Web Service (Data Entry)' button on the Home Page. A pop-up window will appear asking to "Confirm Certificate". Ensure that the correct Digital Certificate is selected and/or displayed, and click '**OK**'.



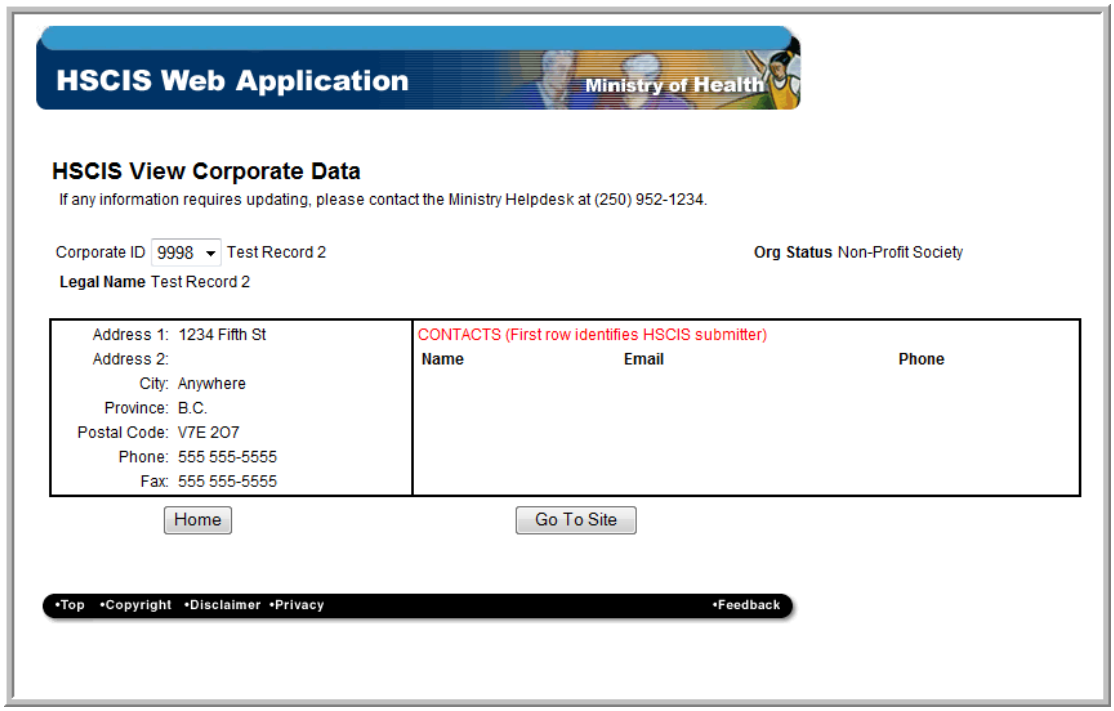
View Org Info

Submission Frequency: This should be reviewed on a regular basis to ensure your organization information (name, address, contacts) is correct and current. If you notice any errors or updates needed, please e-mail Ministry of Health HSCIS Support at **HLTH.HscisSupport@gov.bc.ca** with your Corporate Employer Number and Legal Name in the subject line (i.e. Corp #1234 Smith Ltd.) and details in the body of the message.

In HSCIS, the term 'Corporate' refers to the legal, organizational body that is registered with the Companies Registry. A 'Site' refers to one or many facilities that may be run by the 'Corporate' body in the provision of services. (E.g. "Silvercare, Inc." runs three care facilities named "Silvercare East", "Silvercare West" and "Silvercare Central". In HSCIS, Silvercare, Inc. is the 'Corporate' body, where most of our correspondence is sent, and Silvercare West, East and Central are 'Sites', run by the Corporation.)

There are two screens in this set, identified by the titles **HSCIS View Corporate Data** and **HSCIS View Site Data**.

When you are presented with the **HSCIS View Corporate Data** form (as shown below), a list of corporations to which you are permitted to access will be attached to the Corporate ID field. Once you select one of the entries from the dropdown list, the remainder of the screen will be automatically populated for you with our current information.

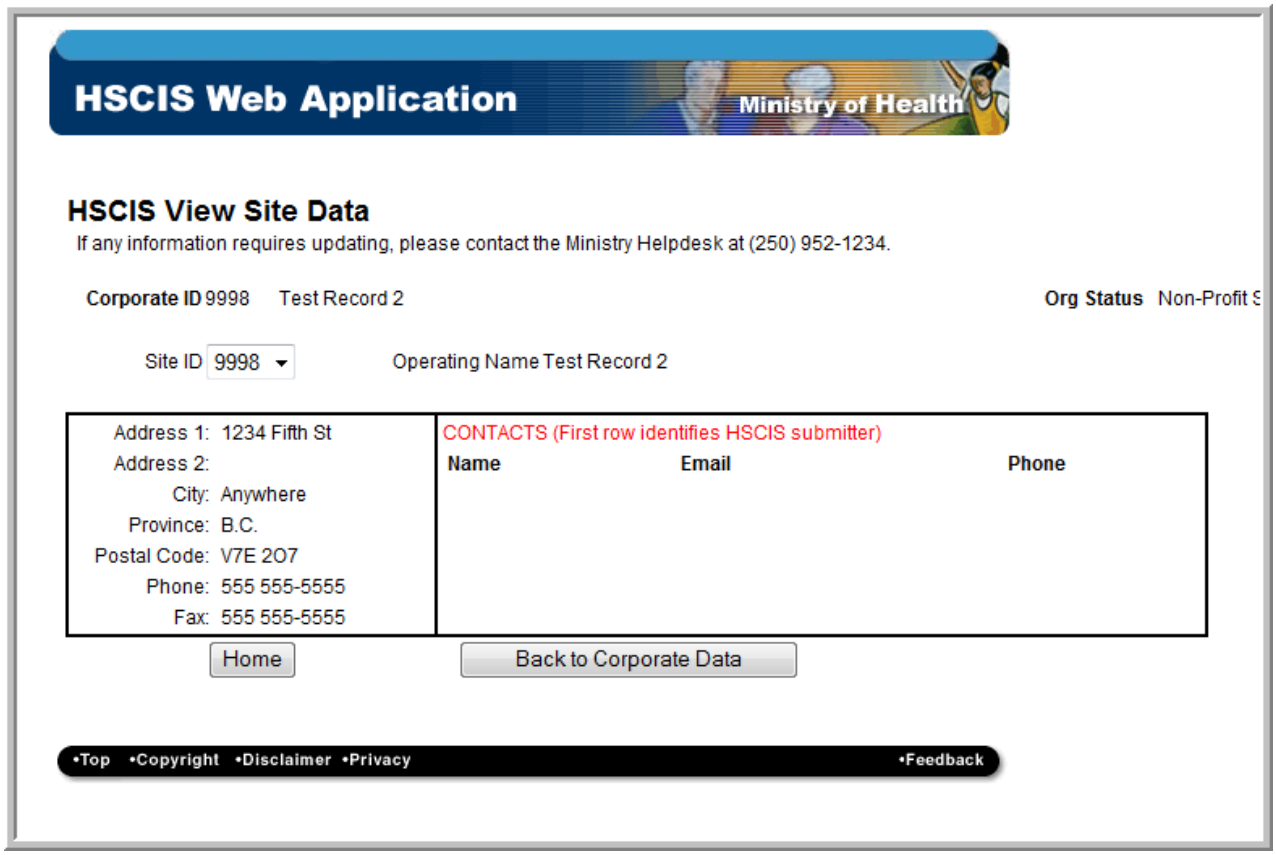


If you are permitted to access multiple corporations and are not sure of the Corporate ID for a specific one, you can refer to HEABC's listing on their web site at (http://www.heabc.bc.ca/userfiles/HTML/nts_2_1533_1.html). If you want to look up the Corporate Number, Site Number, Legal Name or Operating Name, you can refer to HEABC's up to date listings on their web site at (http://www.heabc.bc.ca/public/hscis/pdf/MembersbyCorpIDSEN.pdf). If you have any other questions, you can request the information via e-mail from Ministry of Health HSCIS Support at **HLTH.HscisSupport@gov.bc.ca** with your Legal Name in the subject line (i.e. Smith Ltd.) and details in the body of the message.

Selecting the **Home** button will return you to the Main Menu screen.

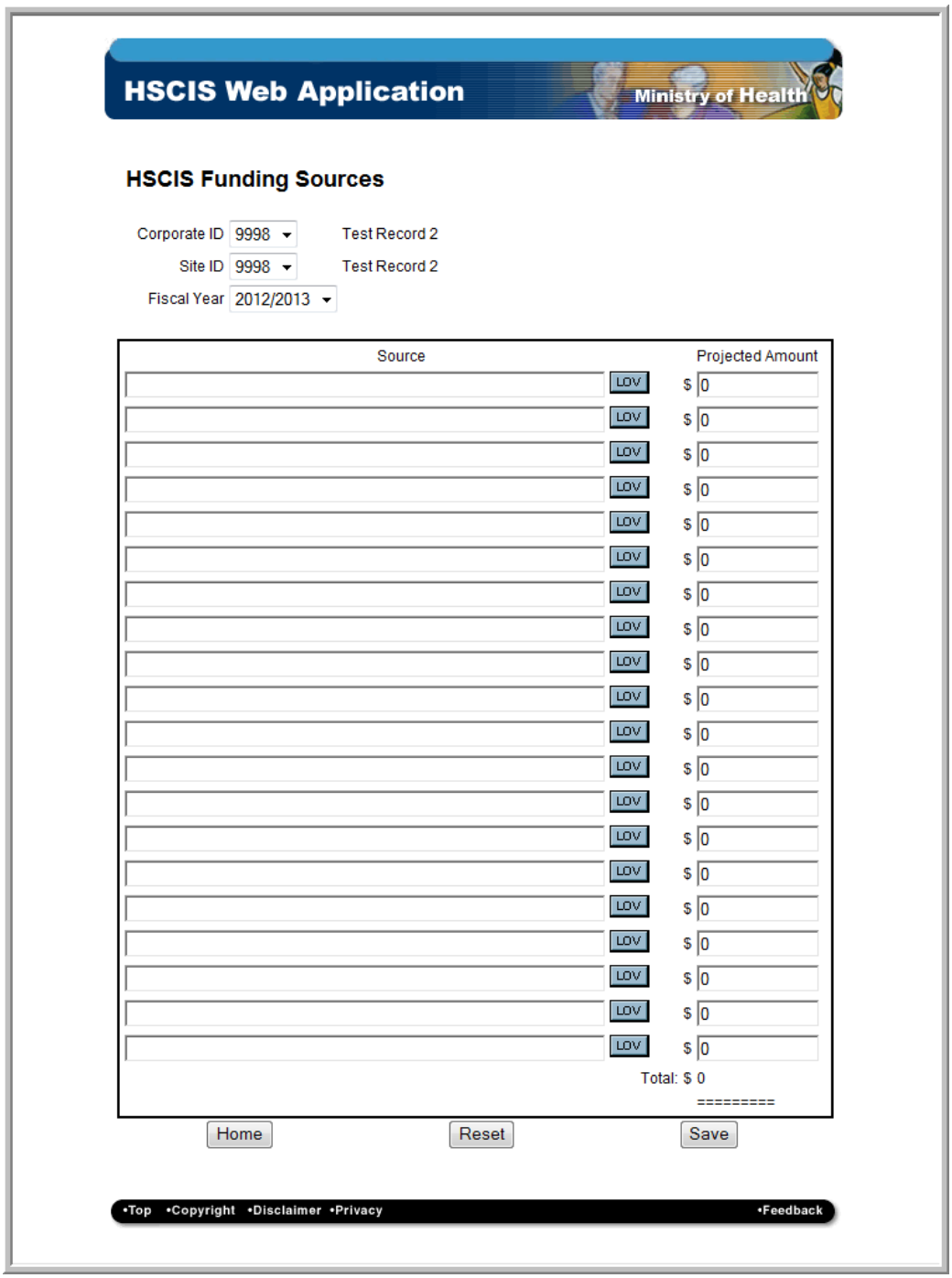
If a Corporate organization is running more than one site, they can use the **HSCIS View Site Data** screen to view the currently stored information regarding the name, address, or contacts at those sites. This can be accessed by pressing the **Go To Site** button at the bottom of the screen.

The **HSCIS View Site Data** form is used to review the name, address or contact information at the various sites run by the organization.



Enter Funding Sources

Submission Frequency: Annually, by July 31st. If there are significant changes in the sources or amount of funding you receive during the year, you may 're-submit' this report at any time Required information is the same; the only change is that you are able to view the organization information in the HNfile application now.



On this screen, you identify all monies you receive from ***all sources*** for the current fiscal year. Fiscal years for the Ministry run from April 1st to March 31st, and so are identified as 2010/2011, 2011/2012, etc. Each line (after Fiscal Year) represents a single source of funding.

For the **Funding Sources** screen, the fields are filled in as follows:

Field	Content
Corporate ID	From the dropdown list, select the Corporation for which you are providing information. Once selected, the legal name of the Corporation will appear to the right. Note: Only entries from the dropdown list may be selected. The options available are based on the registration information provided.
Site ID	Once a Corporate ID is selected, the Site ID dropdown list will be populated with all Sites available within that Corporation. Select the one you are reporting for from the list. Note: In HSCIS, a Site ID that is the same as the Corporate ID identifies the information related to the Corporation as a whole. Thus, if you wish to report Funding Sources for the entire Corporation (rather than site by site), select the Site ID that is equal to the Corporate ID.
Fiscal Year	From the dropdown list, select the Ministry fiscal year for which you are reporting your funding sources (i.e. 2010/2011, 2011/2012, etc.). After the Fiscal Year has been selected, the rest of the screen will be populated with the information from our database. You may make changes as required. **Note:** The database stores this as a single 'snapshot' for each fiscal year. So, if there are changes, all entries (including ones unchanged, must be included on this screen.)
Source	Select each of the appropriate funding sources from the drop list of values (LOV). If it is unclear which funding source should be selected, please e-mail Ministry of Health HSCIS Support at **HLTH.HscisSupport@gov.bc.ca** with your Corporate Employer Number and Legal Name in the subject line (i.e. Corp #1234 Smith Ltd.) and details in the body of the message.
Projected Amount	Fill in the amount of money you are expecting during the fiscal year period. Enter dollar amounts only, no cents. **Please do not include dollar signs ($), decimal points or commas.**

Once the information is complete, select the **Save** button at the bottom of the screen to update the database. A message will be displayed to tell you the information has been successfully saved. Then press the **Home** button to return to the Main Menu.

Change Password Screen

The **Change Password** Screen is used to change your password. You will be requested to change your password the first time you access HNFile.

The following rules apply to passwords:

- Passwords must be six or more characters long.
- Passwords must contain at least one letter.
- Passwords must contain at least one non-letter character.
- Password re-use is not allowed.
- Passwords must be changed every 42 days.

Using the Change Password Screen

Enter your existing password in the *Old Password* text box.

1. Enter your new password in the *New Password* text box.
2. Re-type your new password in the *Confirm New Password* text box.
3. Select the '**Start Over**' push button if you have made an error and wish to re-enter the information.
4. Select the '**Change Password'** push button to change your password.

A message will be displayed indicating that the change of password was successful or identifying the error (i.e., the new password does not conform to the password rules or the New Password and Confirm New Password are different).