

# HDPBC Training and Education

## **HDPBC Importing Cohort Data**

Version: V1.1

Updated: June 2022

## Overview

This document explains how to import cohort data that may include sensitive personal information into the HDPBC Desktop.

This process will load data to the HDPBC SQLServer database so that it can be linked with other data, including HDPBC tokenized/encrypted columns such as PHN. All project team members will be able to access the imported cohort data.

1. Complete the HDPBC [Importing Cohort Data Information Checklist](#).
2. Determine if your organization is already set up to transfer data to HDPBC.
3. Create your SFTP key pair (public and private keys).
4. Submit a request to import cohort data using the HSIAR Request Management System (HSIAR RMS).
5. Receive an HDPBC encryption key.
6. Prepare data for upload.
7. Use SFTP client to transfer your data to HDPBC.
  - a. Install an SFTP client (if needed).
  - b. Transfer files to HDPBC using SFTP.

### Notes:

- The information being imported into the HDPBC Desktop will be reviewed by HDPBC.
- Please ensure you have permission to access this data and permission to have it sent to HDPBC.

## Contents

Overview .....	2
Importing Cohort Data .....	4
Step 1: Import cohort data information checklist .....	4
Step 2: Determine if your organization is already set up to transfer data to HDPBC.....	4
Step 3: Create your SSH key pair .....	1
Step 4: Submit a request to import cohort data .....	1
Step 5: Wait to receive an HDPBC encryption key .....	2
Step 6: Prepare your data for upload .....	2
1. Compress your data .....	2
2. Install encryption software .....	2
Import Encryption Key .....	3
Encrypt Data Cohort Files .....	3
Step 7: SFTP Configuration .....	4
Step 8: Use SFTP to Transfer Your Files .....	4
Step 9: Notify HDPBC that the file transfer is complete .....	6
Document History .....	7

## Importing Cohort Data

### Step 1: Import cohort data information checklist

The HDPBC Importing Cohort Data Information checklist is a required document that ensures HDPBC has all necessary information to import your data cohort and link it to the correct project(s).

Download and complete the HDPBC Importing Cohort Data Information Checklist that is available using [this link](#). You will share the completed checklist with HDPBC in Step 4.

Online learning platform link: [Importing Cohort Data: Step 1: Importing cohort data information checklist \(gov.bc.ca\)](#)

### Step 2: Determine if your organization is already set up to transfer data to HDPBC

Contact the HDPBC Front Desk at [MoHanalytics@gov.bc.ca](mailto:MoHanalytics@gov.bc.ca) and they will determine if your organization is set up to transfer data to HDPBC. They will find the information for you and guide you through the rest of the process.

If your organization is already set up to transfer data to HDPBC, you will not need to create your own SSH key pairs. You will be able to transfer data to HDPBC using existing processes.

Continue with the following steps if your organization is not set up to transfer data to HDPBC.

#### Notes:

Secure File Transfer Protocol (SFTP) creates a layer of protection for data being transferred. It encrypts data using SSH key pairs so that it can be shared between two parties in a protected pathway.

A Secure Shell Protocol (SSH) key pair is created to encrypt data for data transfer. The process creates a private key and a public key. The current holder of the data uses the private key to encrypt the data, and the receiver of the data will be given the public key to be able to decrypt the data. SSH key pairs are created to enable secure data transfers. Windows has a utility that can generate SSH key pairs.

### Step 3: Create your SSH key pair

You will generate an SSH key pair with HDPBC so it can be registered on the SFTP server.

The HDPBC Front Desk at [MoHanalytics@gov.bc.ca](mailto:MoHanalytics@gov.bc.ca) will guide you through setting up the SFTP transfer process.

In this step, you will create a private SSH key and a public SSH key. The public SSH key will have a **.pub** file name extension. You will share your public SSH key with HDPBC when you submit your cohort data import request in Step 4.

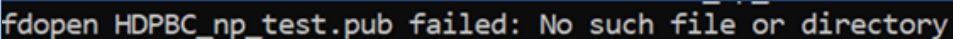
More information on [SSH protocol](#) and [SSH public key authentication](#).

You will start a command prompt from the desktop icon or by the start button, then you will be given specific text to type into the command prompt. This text will create a new SSH key folder, change the directory to the new folder, allow you to enter a file name, and prompt you to enter a passphrase. A passphrase helps protect the keys from unauthorized use.

It is recommended that you name the keys in the following format:  
**"HDPBC\_firstname\_lastname"**.

#### **If you get an error:**

If you see an error like that shown in Figure 1 and the generated .pub file is empty, you may need to try the operation again. When trying again, do not specify a file name when prompted.



```
fdopen HDPBC_np_test.pub failed: No such file or directory
```

Figure 1. SSH key creation error message.

You can rename the files after they have been created to follow the convention "HDPBC\_FirstName\_LastName".

### Step 4: Submit a request to import cohort data

Submit a request to import cohort data by attaching your completed HDPBC Data Cohort Information Checklist and your **public** SSH key to an HSIAR RMS General Inquiry request.

[HSIAR Request Management System](#)

Please reference the HDPBC [Submitting a General Inquiry document](#) for instructions on how to use the HSIAR RMS to submit a general inquiry request.

After submitting a request to import data, you can use the HSIAR RMS system to track the progress of your request.

**Note:**

The HDPBC Front Desk will inform you if you are affiliated with an HDPBC Data Contributor, an organization that makes their data available to HDPBC. If you are, the rest of this process should be completed by IT support who can access the SFTP information from past HDPBC data imports.

## Step 5: Wait to receive an HDPBC encryption key

Following review of your general inquiry request, the HDPBC technical team will register your SSH key so that you can send data to HDPBC using the Secure File Transfer protocol (SFTP).

HDPBC will email you an encryption key that you will need to use to prepare your data. You can track the progress and request updates on obtaining your encryption key using the HSIAR RMS.

**Note:**

The encryption key sent to you is different than the encryption you created with the SSH key pairs, providing a second layer of security to your data. The SSH key pair uses encrypted keys to establish secure communication between you and HDPBC, while the encryption key that HDPBC sends you secures the data itself. These two layers of encryption are used for different parts of this process to ensure a secure data transfer.

## Step 6: Prepare your data for upload

The data cohort must be compressed and encrypted with the key sent to you by HDPBC before being sent to HDPBC to keep it secure while in transit and at rest.

### 1. Compress your data

Compressing your data involves creating a compressed (zipped) folder.

### 2. Install encryption software

The next step in the process is to install encryption software. While there are many tools that you can use to encrypt your data cohort files, one freely available tool is Gpg4win. You can navigate to [gpg4win.org](http://gpg4win.org) and download the software.

**Note:**

You may be required to download this software from your organization's software center.

## Import Encryption Key

To import the encryption key, you will need to open the Kleopatra utility included in the Gpg4win software distribution. Using Kleopatra, you can import the file you received from HDPBC containing your HDPBC encryption key.

A certification dialogue box will pop up that you will need to say **No** to.

If the process was successful, you should now see the key has been imported (see Figure 2).

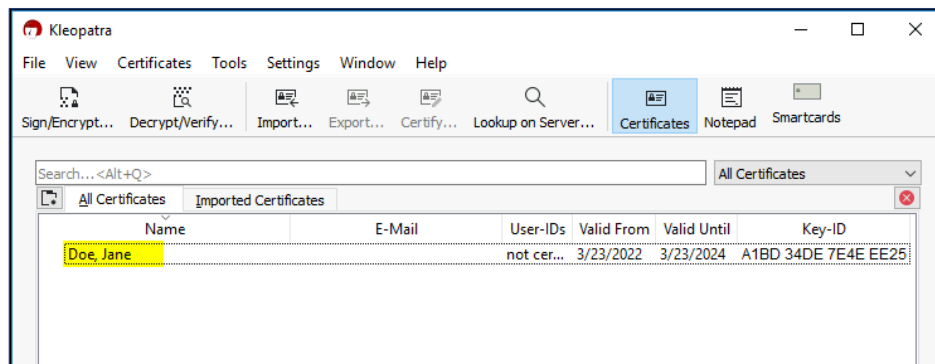


Figure 2. If successful, you will see the key listed.

## Encrypt Data Cohort Files

The next step is to encrypt the data cohort files. This is done by selecting the file(s) in the Windows file explorer. You should right-click on the file(s) and select 'Sign and encrypt'.

You will be presented with the Kleopatra "Sign/Encrypt" dialogue box. In this box, you will uncheck the 'Sign as' and 'Encrypt for me' boxes and check the 'Encrypt for others' box.

Another dialogue box, the certification selection, will be presented. You will choose the key you've imported from HDPBC and click **OK**. If you are presented with an "Encrypt" option, do so. An "Encrypt-to-Self" warning will appear, which you can press **Continue** on to move on with the process.

When the encryption is complete, you will get a message that all operations are complete. Click **Finish**.

You should see the encrypted (.gpg) version of your compressed (.zip) file. This file is now ready to be sent to HDPBC via SFTP.

## Step 7: SFTP Configuration

Since the data has personal information, you will need to send it via a properly configured Secure File Transfer Protocol (SFTP) server. SFTP servers create a secure connection for data transfers, permitting a high level of security and protection for the data being transferred.

### Note:

You may need Administrator privileges on your desktop to complete the installation.

You will need to install SFTP Client. To do this, navigate to <https://filezilla-project.org> and click **Download** from the left-hand navigation menu (Figure 3). At this point, you will complete the download and installation steps relevant to your operating system.



Figure 3. FileZilla page. Press the highlighted **Download** button.

## Step 8: Use SFTP to Transfer Your Files

In FileZilla, you can click the button at top left (see Figure 4) to start a new connection.

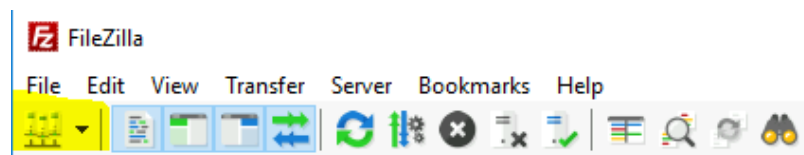


Figure 4. Click the highlighted button to start a new connection.

You will be prompted to fill in the connection information (see Figure 5). It should be completed as specified in Table 1.



Protocol	SFTP
Host	For users on a Health Authority network device: 10.57.149.10 For users outside HA networks (firewall modification): <i>sftpsvcs.healthbc.org</i>
User	<your username> e.g., jane.doe
Key File	1. Click <b>Browse...</b> Navigate to the private key file you created (the file <u>without</u> the .pub extension, e.g., NOT: HDPBC_firstname_lastname.pub) 2. In <b>Logon Type</b> select <b>Key File</b>
Port	Leave blank

Table 1. Connection information for FileZilla.

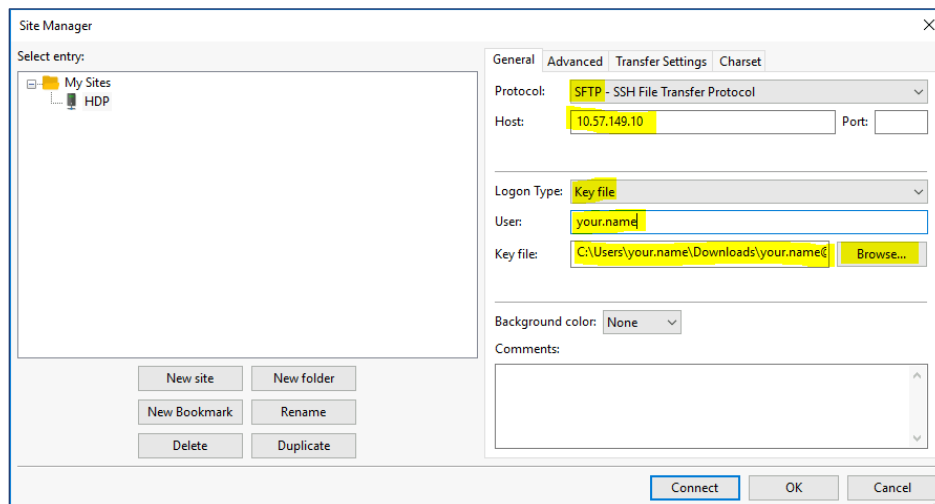


Figure 5. Enter the information as provided in the table above into the highlighted areas.

When you click **Connect**, you may see an “Unknown host key” error. If this happens, you can click **OK** to accept the warning.

If you are successfully connected, the “Remote site” panel to the right will be populated with the folders you have access to.

In the “Local site” pane on the left side of the page, you can navigate to the folder that contains your encrypted (.pgp) file. You need to drag the encrypted file from the **Local site** to the **Remote site** on the right side of the page (Figure 6).

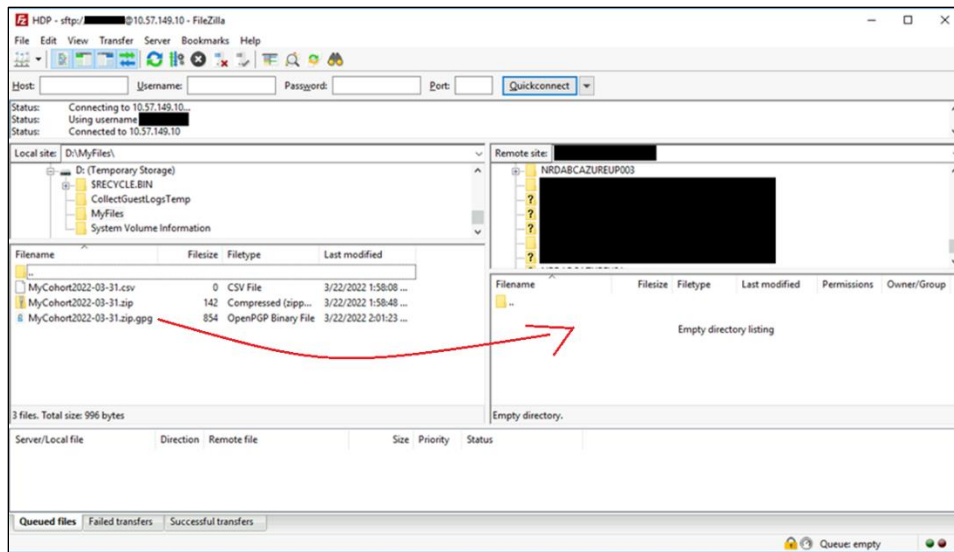


Figure 6. Drag your encrypted folder from the local site to the remote site.

If the file was transferred successfully, you will see the file appear in the 'Remote site' on the right side of the window, and the 'Successful transfers' tab at the bottom of the window will show details about the transfer (Figure 7).

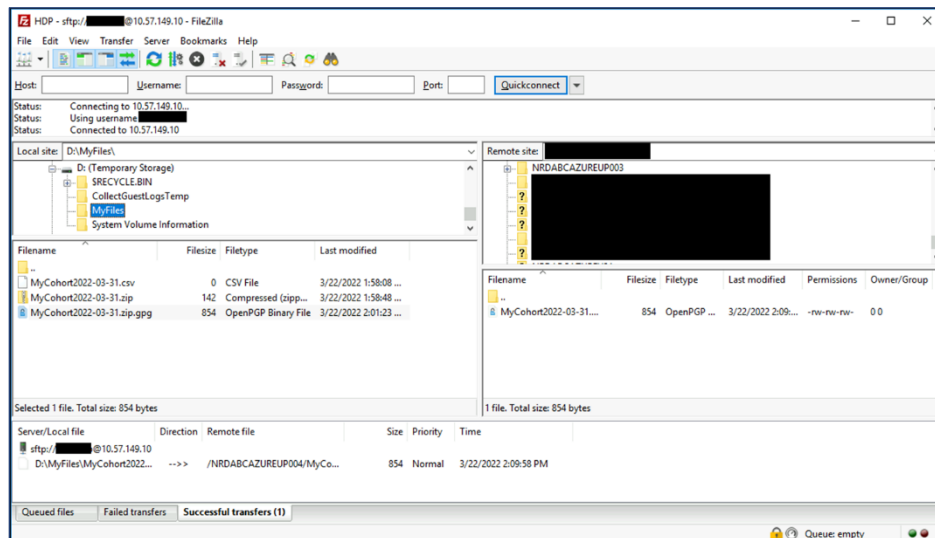


Figure 7. The "Successful Transfers" tab will show details about the transfer.

## Step 9: Notify HDPBC that the file transfer is complete

Open the HSIAR RMS and update the HSIAR RMS ticket to notify HDPBC that file has been transferred. Include the folder and file name.

## Document History

Version	Table Heading	Author	Changes
1.0	23-Mar-2022	HDPBC Team	Draft initial version
1.0	25-Mar-2022	HDPBC Team	Content edits
1.0	9-May-2022	HDPBC Team	Content edits
1.1	12-June-2022	HDPBC Team	Formatting edits