Shared health
Soins communs
Manitoba

How to Encrypt Files

As part of the registration process or after registration, some Home Clinics will submit Primary Care Data Extract (PCDE) files to Manitoba Health on a CD or USB. PCDE files contain Personal Health Information (PHI), and the Personal Health Information Act (PHIA), requires that the data be secured before submission. This document provides instructions for encrypting files.

Minimum Technical Requirements

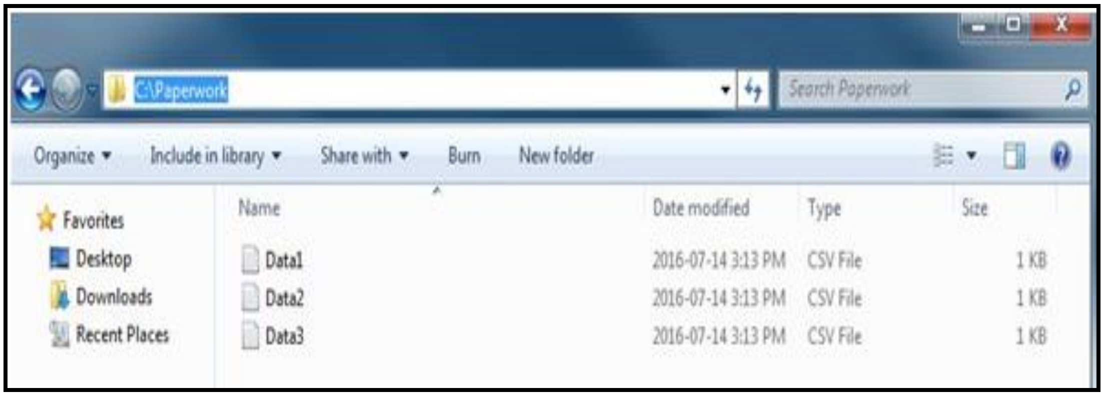
To encrypt files, Home Clinics must use a computer that meets the following requirements.

Software	Hardware
7-Zip 16.02 (2016-05-21) for Windows or greater. The installer for both 32-bit and 64-bit Windows can be found at: http://www.7-zip.org/download.html *If you are unsure which version of 7-Zip to install, please contact your IT Support to confirm*.	• Kingston DataTraveler Vault 3.0 USB Drive **or**; • CD Drive

Step 1: Locate files to be encrypted

Use **Windows File Explorer** to find the folder location that contains the PCDE files requiring encryption.

In the example below, all files are located at C:\Paperwork



Name	Date modified	Type	Size
Data1	2016-07-14 3:13 PM	CSV File	1 KB
Data2	2016-07-14 3:13 PM	CSV File	1 KB
Data3	2016-07-14 3:13 PM	CSV File	1 KB

Step 2: Select the files to encrypt

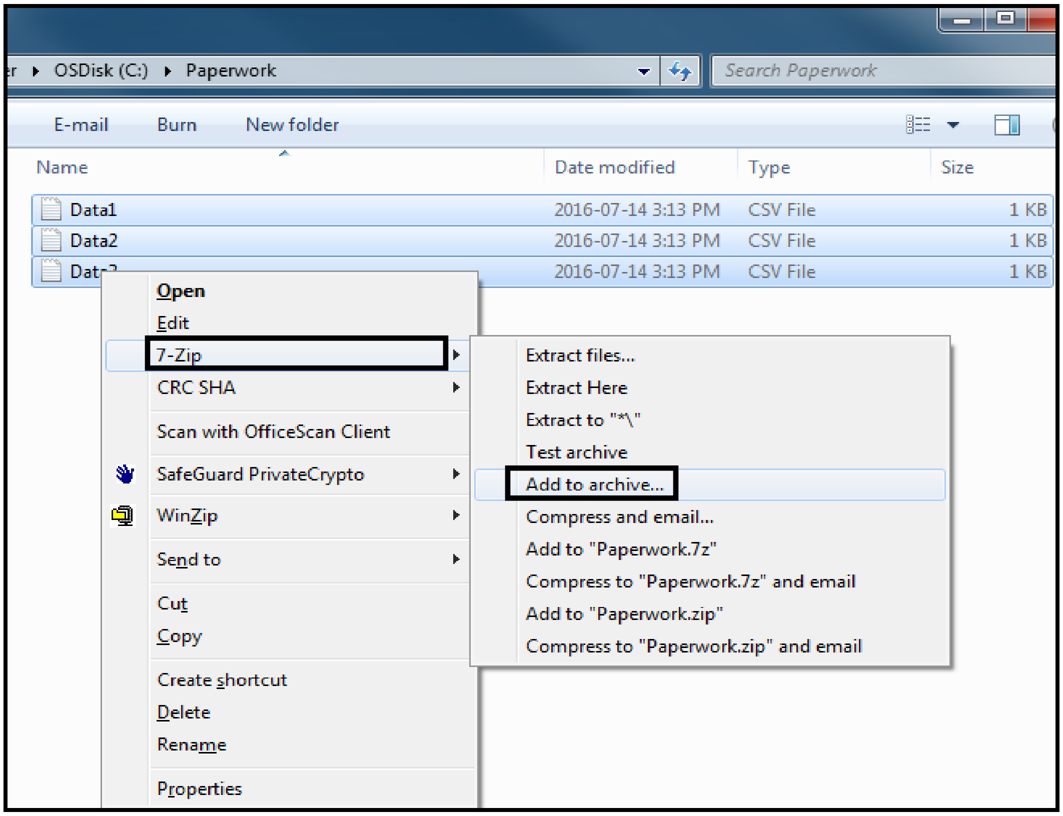
Select each of the Primary Care Data Extract files you want to transmit to Manitoba Health.

- Select all files to encrypt
- Right click on the selected files
- Select **7-Zip** from the menu
- Select **Add to archive**

These steps are illustrated below

Tip

To select more than one file, hold down the **Ctrl** key and click on all the files you would like to encrypt. Release the **Ctrl** key once you are finished selecting files.

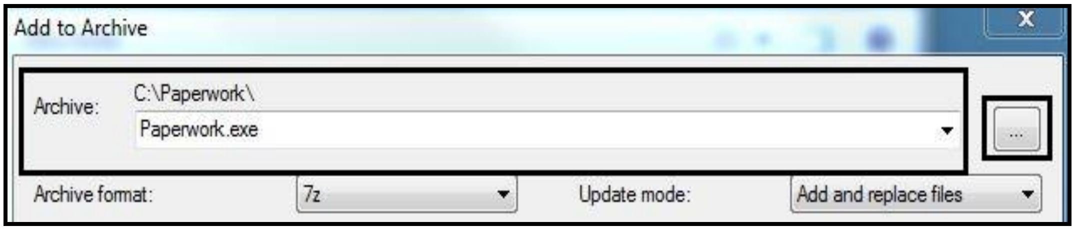


Name	Date modified	Type	Size
Data1	2016-07-14 3:13 PM	CSV File	1 KB
Data2	2016-07-14 3:13 PM	CSV File	1 KB
Data3	2016-07-14 3:13 PM	CSV File	1 KB

Step 3: Configure self-extracting Zip file

Once you have selected the **Add to Archive** option, a pop up window will appear. At the top of the window there is a section labelled **Archive**. This is where you define where the encrypted files will be stored and the file name.

- Click on the eclipses button (...) that is to the right of the text box. This will allow you to use Windows Explorer to select the desired storage location.



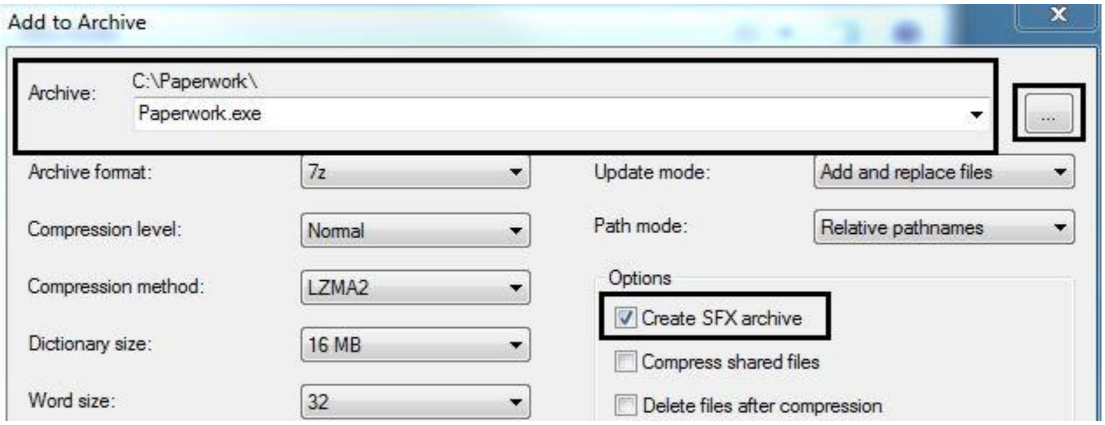
Add to Archive

Archive: C:\Paperwork\
Paperwork.exe

Archive format: 7z

Update mode: Add and replace files

- Check the box next to **Create SFX archive**



Add to Archive

Archive: C:\Paperwork\
Paperwork.exe

Archive format: 7z

Update mode: Add and replace files

Compression level: Normal

Path mode: Relative pathnames

Compression method: LZMA2

Dictionary size: 16 MB

Word size: 32

Options

☑ Create SFX archive

□ Compress shared files

□ Delete files after compression

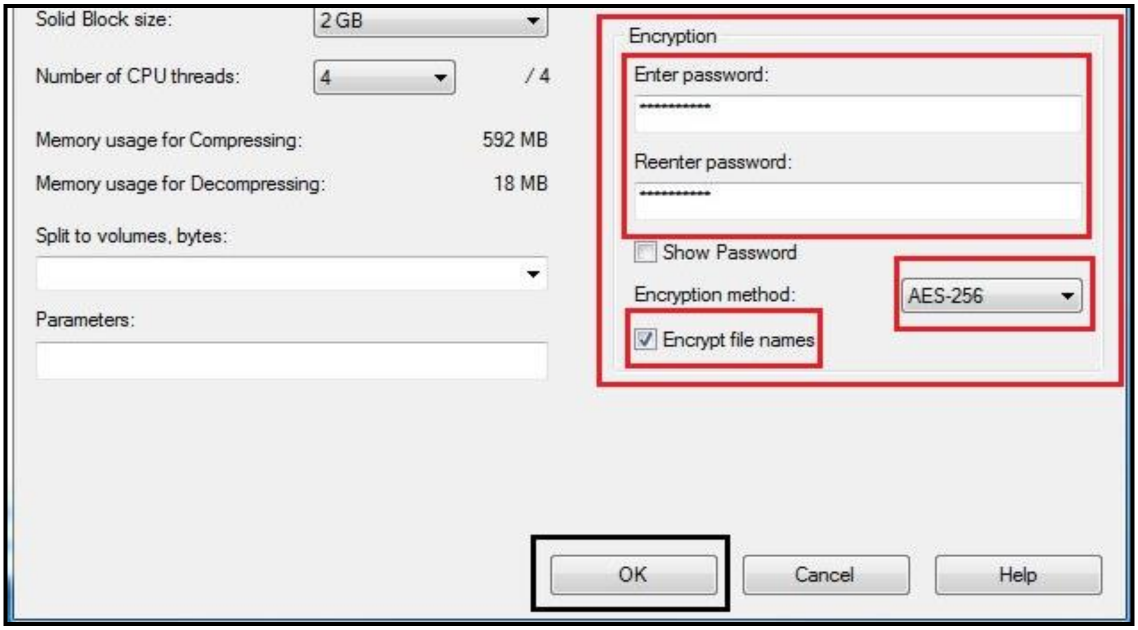
Step 4: Encrypt the File:

When selecting a password, consider the following requirements:

- The password must be at least 8 characters long and contain each of the following:
    - one lower case character (a-z)
    - one upper case character (A-Z)
    - one number character (0-9)
- Select **AES 256** as the Encryption Method
  Note: file(s) will be rejected if this format is not selected
- Check the box next to **Encrypt file names**
- Click **OK**

Tip

The data will need to be decrypted once it is received. If necessary; note the password somewhere secure so that you can provide it to the data recipient via email (EMRInfo@gov.mb.ca).



Solid Block size: 2 GB

Number of CPU threads: 4 / 4

Memory usage for Compressing: 592 MB

Memory usage for Decompressing: 18 MB

Split to volumes, bytes:

Parameters:

Encryption

Enter password: ***********

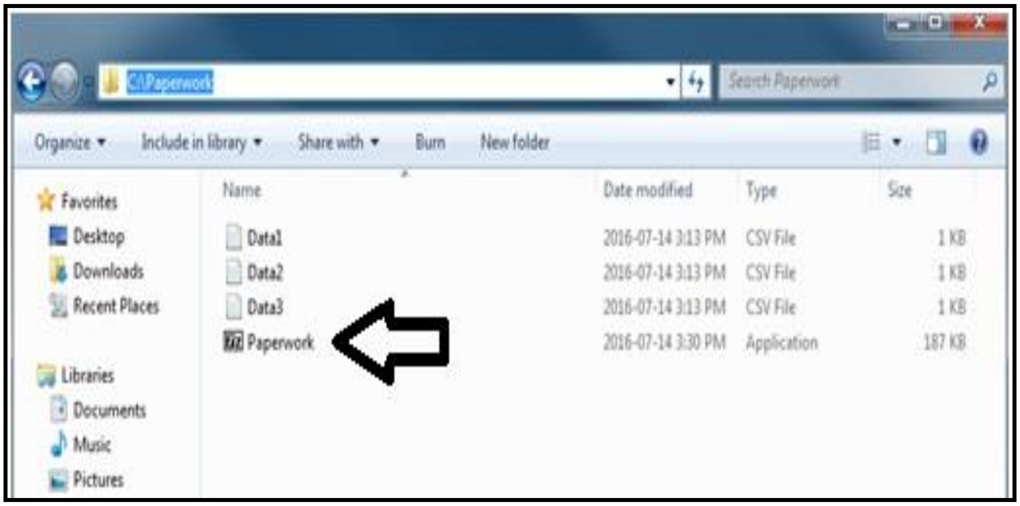
Reenter password: ***********

□ Show Password

Encryption method: AES-256

☑ Encrypt file names

- The resulting **.exe file** will appear in the destination folder you selected in Step 3 above

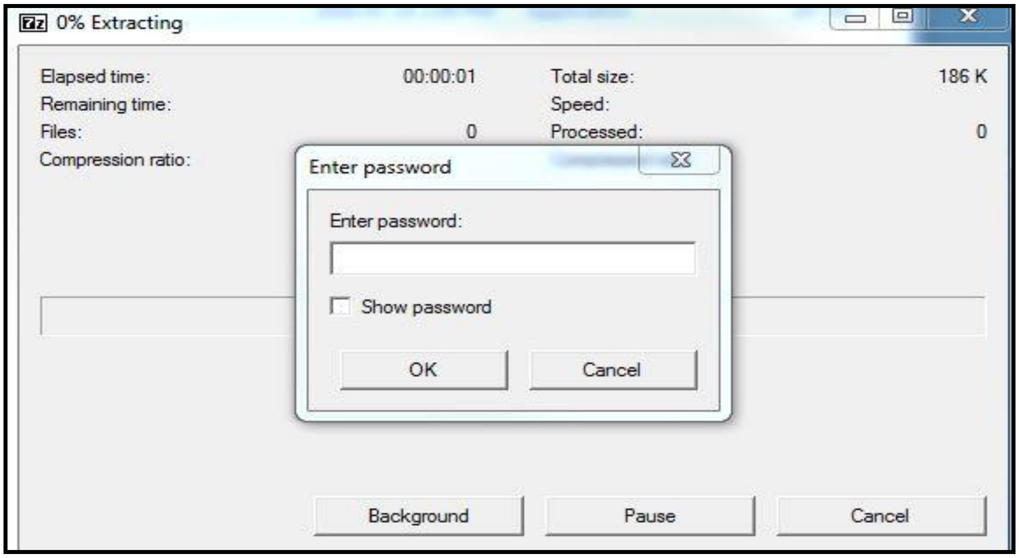


Name	Date modified	Type	Size
Data1	2016-07-14 3:13 PM	CSV File	1 KB
Data2	2016-07-14 3:13 PM	CSV File	1 KB
Data3	2016-07-14 3:13 PM	CSV File	1 KB
Paperwork	2016-07-14 3:30 PM	Application	187 KB

Step 5: Test the Files:

Please **ensure that the file produced** works properly by:

- copying the file to a temporary location
- open the **.exe** file, select **Extract** and enter the password to extract all the file(s)
  - If you were not asked to enter a password, recreate the file, ensuring that you provide a password in Step 4



Elapsed time: 00:00:01
Total size: 186 K
Remaining time:
Speed:
Files: 0
Processed: 0
Compression ratio:

Once you have entered your password and pressed **OK**, if there is a message indicating the file is corrupt and cannot be extracted, or if the resulting files in the directory are not the files that you intended to encrypt and send, then something has gone wrong, please go back to **Step 3** and repeat the process.

Step 6a: Flash Drive Users:

- Insert the Kingston DataTraveler Vault into your computer's USB port
- A new log in window will pop-up and ask for a password
- Select a password that is different from the password that you used to encrypt your data files and type it into the Password text box of the DataTraveler Vault

- If you are using a new USB Flash Drive, please follow the video instruction below:

https://www.youtube.com/watch?v=E8zy0LRAOIY

Tip

This password will be required before any user can access the data files. If necessary; note the password somewhere secure.

Step 6b: Copy Files - Flash Drive Users:

- Copy (drag and drop) the .exe files to the Flash Drive
- Ejecting the USB:
  - On the right bottom of your monitor, click the Kingston icon. There you will see an option which allows you to Shut down DTVault Privacy. Click **OK.**
  - Once the "DTVault Privacy can now be safely removed from the system" message is presented, you can safely remove the USB flash drive.

Step 7: Copy File(s) - CD Users:

- Put your CD drive in your desktop (or laptop) disc tray and copy the .exe files to the disc.