IDHS Encrypting Data for file transfer

1. **Document Information**	
Document Name	IDHS-Encrypting-Data-for-file transfer-v1.docx
Service	Identifiable Data Handling Solution (IDHS)
Author	Bhavesh Varsani (BV)
Contributors	Kristina Drew (KD)
Issue Date	22/07/2013

2. **Document History**		
Version	**Date**	**Summary of change**
1.0	28/05/2013	First Draft

Contents

3 Introduction

The purpose of this document is to provide guidance on data encryption and principles of transferring sensitive data such as patient identifiable data (PID).

Any files containing sensitive data should be encrypted for storage and transit. A strong encryption method that includes a password should be used.

Once encrypted, the files can be transferred to the respective research groups using the IDHS Service which is specifically designed for file transfer and handling of identifiable data.

4 Pre-requisites

4.1 Application requirements

For the purpose of this document “7Zip” is used as encryption product for encrypting and decrypting data. 7Zip is:

- An open source compressed archive tool which will also encrypt files
- Available on the SLMS desktop
- Can be downloaded from www.7-zip.org

5 IDHS secure transfer process

5.1 Overview

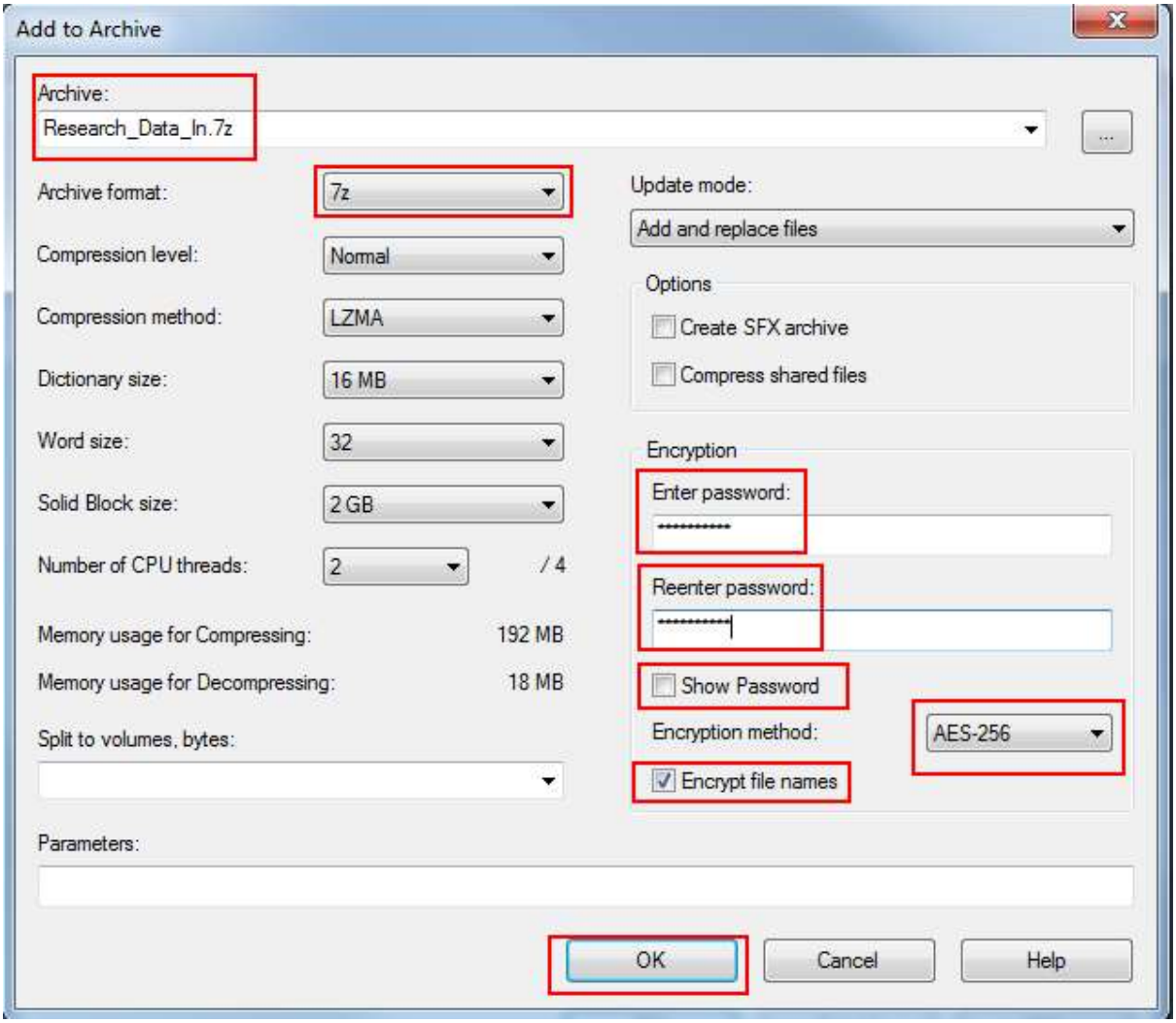
- Both parties agree a password to be used when encrypting the file(s) to be transferred
- Data provider uses 7Zip to compress and encrypt the file(s) to a secure archive
- Data provider uses IDHS Service to upload the encrypted archive ready for collection by the recipient from the respective research group
- Data recipient accesses the IDHS service.
- Data recipient decrypts the encrypted data using the agreed password

5.2 Encryption

1. (Both parties) Agree passwords for encryption this should be communicated at the outset. When using the IDHS service to transfer encrypted files, the password can be communicated using different mechanisms (e.g. by phone, email, standard post or face-to-face)

- (Data provider) Use 7Zip to compress and encrypt file to a secure archive
    a. Highlight file(s) to be transferred.
    b. Right click on selected files or folders. (“Research_Data_In” in this example)
    c. Select **7-Zip** option
    d. Select **Add to archive…**
    e. Use the default **.7z** archive format that utilises a strong encryption method called **AES-256**

f. Ensure the **Encrypt file names** is ticked
g. Ensure the **Show Password** is unticked
h. Use a strong password
   Advice:
   i. UCL passwords policy
   http://www.ucl.ac.uk/isd/common/registration/passwords/faq/acceptable_password
   ii. Password generating websites. Example
   http://www.random.org/passwords/



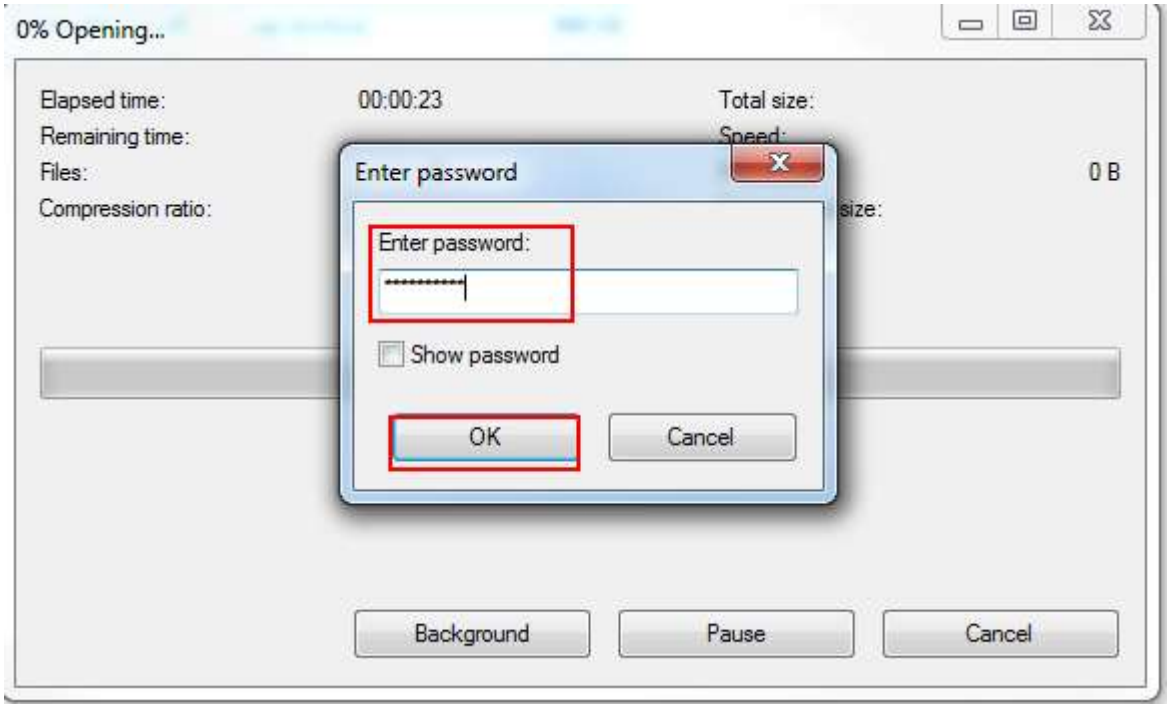
- (Data provider) logs into the IDHS file transfer service to transfer files
  - In your web browser go to the file transfer gateway https://filetransfer.idhs.ucl.ac.uk
  - Logs in with their IDHS account
  - Uploads the encrypted content to the relevant research group

5.3 Decryption

Once documents uploaded /sent, the data provider will pass the password over to the data handler for them to decrypt the data once they receive it.

To Decrypt:

- (Data Receiver) Moves the received files from the Research Group space in MFT Arrivals to the same Research group space in Group Data
- Use 7Zip to decrypt file / folder
    a. Highlight file(s) to be transferred
    b. Right click on selected files or folders.
    c. Select **7-Zip** option
    d. Extract to “FileName\” where Filename is the name of the encrypted file. In this case it would be “Research_Data_In\”
    e. Enter the password provided by the **data sender** and click on OK



End of Document