Team Name: Health Information Services Team Lead: Manager – Health Information Services Approved by: Regional Lead – Corporate Services & Chief Financial Officer	Reference Number: ORG.1410.SG.001 Program Area: Health Information Services Policy Section: Health Information
Issue Date: January 15, 2024 Review Date: Revision Date:	Subject: Encrypting Records using 7-Zip File Manager

Use of pre-printed documents: Users are to refer to the electronic version of this document located on the Southern Health-Santé Sud Health Provider Site to ensure the most current document is consulted.

STANDARD GUIDELINE SUBJECT:

Encrypting Records using 7-Zip Manager

PURPOSE:

To provide a guideline for compressing and encrypting, with password protection, confidential information for email transfer.

DEFINITIONS:

PDF - stands for "portable document format". Essentially, the format is used when you need to save files that cannot be modified but still need to be easily shared and printed.

7-Zip File Manager - is a file compression and encryption software that allows employees to send files efficiently and securely within and outside of Southern Health-Santé Sud. This software is often used to package a single file, multiple files, or an entire folder into a passphrase-protected and encrypted package when other options are not available (i.e. Adobe Pro).

Record – A record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, on any storage medium or by any means including by graphic, electronic or mechanical means, but does not include electronic software or any mechanism that produces records. For the purposes of this policy, record(s) and the terms file, folder and documents will be used interchangeably.

IMPORTANT POINTS TO CONSIDER:

Regionally owned devices (i.e. computer) are not deployed with 7-Zip File Manager installed. Staff requiring the use of 7-Zip File Manager can submit a ticket to the service desk. There is no cost associated with the use of the software at the time of the publication of this guideline.

Documents that have been password protected and encrypted using 7-Zip Manager can only be opened by the recipient using 7-Zip Manager.

Larger files or folders will take more time to convert and save.

7-Zip Manager may be used to securely email a medical record requiring a review by the Regional Standards Review Committee, Infection Control, Risk Management or other program as the case may be.

Contact the Privacy and Access Specialist in circumstances where The College of Physician Surgeons or other regulatory bodies make a request to send information to a cloud service.

There is no requirement to protect and encrypt records using 7-Zip manager with the use of a vault privacy USB storage device purchased from the Digital Shared Services approved product list.

Excel files (.xlsx) can be encrypted and password protected using Microsoft Excel. 7-Zip Manager is not required.

Word files (.docx) can be encrypted and password protected using Microsoft Word. 7-Zip Manager is not required.

Follow ORG.1411.PL.101 – Access to Personal Health Information and ORG.1411.PL.502 – Use and Disclose of Personal Health Information when responding to requests for Personal Health Information (PHI).

PROCEDURE:

1 Converting Records to a PDF file

1.1. **Paper Records**

- Locate the record (i.e. medical record or personnel file) and identify the relevant documents (i.e. visit encounter or request for leave).
- Scan the paper record to email (this must be the email of the person scanning the record).
- Name and save the scanned record to a folder in the network ie. H: home drive or program drive.
- Permanently delete the email with the attached scan in PDF format from the inbox and delete box.

1.2. **Electronic Patient Records (EPR) or Business Records**

- Bring into focus the relevant record (i.e. patient record or payroll record).

- Search for the relevant documents.
- Print or save in PDF format.
- Where it is necessary scan and save the printed records following 1.1.
- Where required, name and save the scanned records to a secure folder on the network. These records will be deleted after transfer.

1.3. **Electronic Medical Record (Accuro)**
Refer to departmental instruction.

2 Encrypting Files

2.1. Highlight the relevant record(s), right click and select **7-Zip** and **Add to Archive**

2.2. Change the **Archive format** to “zip”.

2.3. Create a password that is a minimum of 8 characters long and includes one upper case letter, a number and a symbol. Re-enter the password and select **OK**.

3 Sending by Email

3.1. Review the Southern Health-Santé Sud ORG.1411.SG.001 Emailing Confidential Information Guideline to ensure best practices are followed.

3.2. Provide the intended recipient with the password by phone, fax or separate email (where applicable test the email address/confirm fax number).

3.3. Create a new email in outlook.

3.4. Enter the recipient’s email address.

3.5. Select attach file and locate the record(s) recently encrypted (.zip) and double-click to attach.

3.6. Test the security of the document. Double-click on the file to ensure a password prompt appears. Close.

3.7. Confirm the records have been received by the intended recipient.

3.8. Permanently delete the email(s) from the sent box and delete box.

3.9. Permanently delete both formats of the record(s) from the network drive

4 Opening and Unencrypting Files sent by Email

4.1. Double click on the attached .zip file.

4.2. A warning may appear. Click ‘Open’.

4.3. 7-Zip Manager will open.

4.4. Double click the file.

4.5. Enter the password.

4.6. Save the record to a secure location on the network or print.

4.7. Delete the email from the inbox and delete box.

REFERENCES

ORG.1411.SG.001 - Emailing Confidential Information
ORG.1411.PL.101 – Access to Personal Health Information
ORG.1411.PL.502 – Use and Disclose of Personal Health Information