Team Name: Health Information Services Team Lead: Privacy and Access Specialist Approved by: Regional Lead – Corporate Services & Chief Financial Officer	Reference Number: ORG.1411.PL.404 Program Area: Health Information Services Policy Section: Privacy & Access
Issue Date: March 23, 2016 Review Date: Revision Date: December 29, 2023	Subject: Security and Storage of Confidential Information including Transportion

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.

*Words beginning with a capital letter may be found in the definitions.

SUBJECT:
Security and Storage of Confidential Information including Transportation

PURPOSE:
To ensure that recorded Confidential Information will be properly stored, secured, and Maintained in the appropriate manner to protect its confidentiality and integrity.

To ensure the Security and integrity of Confidential Information during transmittal by any means including internal and external delivery networks, voice mail, wireless technology, email and the Internet.

To ensure Confidential Information used within the region is transported in a manner that protects the confidentiality, privacy, security and integrity of that information in accordance with *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act (*PHIA).

BOARD POLICY REFERENCE:
Executive Limitation (EL-02) Treatment of Clients.

POLICY:

- Confidential Information is to be collected, used, disclosed or accessed only by Individuals who are authorized for that purpose. Individuals thus authorized must have a clear understanding of the authority, parameters, purposes and responsibilities of their access, and of the consequences of failing to fulfill their responsibilities.
- Security safeguards shall include both physical and human resource safeguards to prevent unauthorized collection, Use, Disclosure and access of Confidential Information.
- Physical Security measures include such safeguards as locked filing cabinets, restricted access to certain offices or areas, the use of passwords, encryption and lock-boxes. Human resource Security measures include Security clearances, sanctions, training and contracts.
- Security safeguards should incorporate appropriate identification, authentication and information integrity/availability as appropriate.

DEFINITIONS:

Client: means any person (including a Person Permitted to Exercise the Rights of an individual, where the context so requires) who receives health care services within Southern Health-Santé Sud, including patients and residents.

Confidential Information: includes, but not limited to Personal Information (i.e. employee number, personal email account, gender etc.) as defined in FIPPA; Personal Health Information as defined in PHIA; and, administrative records collected and created as part of the course of business of Southern Health-Santé Sud and related to legal, financial and operational matters of a confidential nature.

Recipient: for the purpose of this policy, means Staff of Southern Health-Santé Sud that receive the Confidential Information. The Recipient may also be the Sender.

Record or Recorded Information: 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 graphic, electronic or mechanical means, but does not include electronic software of any mechanism that produces records.

Sender: for the purpose of this policy, means Staff of Southern Health-Santé Sud that arranges for the delivery or transfer of Confidential Information or Staff of Southern Health-Santé Sud that carries or transports the Confidential Information. The Sender may also be the Recipient.

Privacy Breach: means, in relation to personal information and personal health information,

a) Theft or loss; or
b) Access, Use, Disclosure, destruction or alteration in contravention of FIPPA and/or PHIA

PROCEDURE:

- All written Confidential Information will be placed in an appropriately secured file. Paper files (both Client and Staff) containing such information shall be kept in a Secured Place at all times within the resources available other than when being updated or used by authorized personnel as a necessary function of their work.

- Confidential Information stored in an electronic format on a fixed computer, server or terminal shall be properly secured from unauthorized access. Confidential Information stored on electronic media (i.e. camera card or USB drive) shall be kept in a Secured Place at all times and shall be used only by authorized personnel having access to a protected system. Prior to removal from an office, any Confidential Information contained within the computer hardware or an electronic storage media shall be secured or removed.

- Staff who sign on to a computer must not leave the computer without logging off before leaving the workstation. User password protocols must be in place and utilized. Where possible, automatic log offs after a prescribed period of disuse should be programmed for all workstations.

- Radiological and digital images shall be appropriately labeled and kept in a Secured Place at all times other than when required for work purposes by authorized personnel.

- Where information is requested to be saved to a USB, use an encrypted USB storage device purchased from the Digital Shared Services approved product list.
  - Any USB used for the communication, storage and transport of Confidential Information must be provided by Digital Shared Services. The person requesting the information may be responsible for the cost of the USB device.
  - Any USB drive used for the disclosure of Confidential Information must be clearly labelled with “CONFIDENTIAL” and “SOUTHERN HEALTH-SANTÉ SUD”.

- All Confidential Information that is mailed through regular postal service, interdepartmental mail or sent via courier must be marked ‘CONFIDENTIAL’, clearly labeled with the name and address of the intended recipient and have reasonable safeguards put in place to ensure Security and integrity of the information.

- Confidential information that is beyond normal documentation and has a high level of sensitivity (i.e. entire files or original documentation intended to be shared in court, etc.) should be sent either by person, registered mail, express post with signing option purchased, or courier. Whenever reasonable, a photocopy should remain at the originating site if the original documentation must be sent.

- Confidential Information shall not be transmitted via electronic mail without appropriate safeguards such as encryption or transmittal within a secure firewall. See

ORG.1411.SG.001 Emailing Confidential Information and ORG.1410.SG.001 Encrypting Records using 7-Zip File Manager.

- Staff leaving voice messages containing Confidential Information should be discreet. Confidential Information should never be left on a Client's voicemail unless the Client who the information is about has authorized it. Any Confidential Information relayed by voice message must be kept to the minimum required for the purpose of the communication. Staff receiving voice messages containing Confidential Information should listen to the message in private and delete the message as soon as possible. Appropriate password and Security measures should be in place for access to voice mail.

- Fax machines shall be located in a Secured Place where they can be used and monitored only by authorized staff. A Record of Access/Disclosure/Release of Confidential Information, must be attached to all documents stating that the transmittal is confidential and that any unintended receiving party is prohibited from reading or disclosing the information to anyone else, (i.e., a confidentiality caution). Users of fax machines shall follow the Southern Health-Santé Sud Policy ORG.1411.PL.407 Transmission of Personal Health Information via Facsimile Fax.

- Confidential Information in files or electronic media shall be returned to its designated and secured storage location and not allowed to accumulate or be left unattended on desktops or any other location in a non-secured place.

- Everyone dealing with Confidential Information in any manner shall take reasonable precautions to protect Confidential Information from fire, theft, vandalism, deterioration, accidental destruction or loss and any other hazards.

Transportation of Confidential Information Off-site

- All Confidential Information removed from a Secured Place must be traceable in an electronic health system, or manual tracking system.

- If Confidential Information is removed from the Trustee's premises by an authorized person for purposes authorized by the Trustee, that person(s) shall carry the file/electronic media with them or ensure Secure storage at all times. If it is necessary to leave Confidential Information unattended in a vehicle, it must be stored in a Secured Place such as a locked trunk or in an out-of-sight location in a locked vehicle if there is no trunk.

- Staff shall not leave Confidential Information in a vehicle for an extended period of time. Confidential Information shall be kept in a Secured Place until it can be returned to the site it orginated from or securely destroyed.

- All transport containers, must have a label on the outside identifying the container (sealed envelope, zippered bag, etc.) as "Property of Southern Health-Santé Sud, CONFIDENTIAL

INFORMATION. If found, please call (204) _____ (sender's phone number). See ORG.1411.PL.404.FORM.03 Confidential Information Label.

- No Confidential Information shall be transported, stored or left in a location that could result in the destruction or deterioration of the Confidential Information. For example, radiological images or a USB drive could be destroyed if left in a locked trunk on a hot day and paper Records could be destroyed if left by an open window during a rainstorm.

- Prior to transport of Confidential Information off-site, consider the following:
  - Confidential Information should be removed off-site only when absolutely necessary;
  - Confidential Informatin removed off-site should be retricted to the minimum amount required to accomplish a task or service;
  - Whenever practical, only copies of a Record should be taken off-site; and
  - The tracking sytem used can clearly identify the type of Confidential Information transported, the person the Confidential Information is about, the sender and recipient.

- The Sender of Confidential Information shall maintain, or have access to, a list of the Confidential Information and the Client(s) or persons the information is about that is being transported. This may be in an electronic health system and/or system generated report (i.e. schedule).

- Southern Health-Santé Sud ORG.1411.PL.404.FORM.01 Tracking of Confidential Information Worksheet or ORG.1411.PL.404.FORM.02 Tracking-Transport-Confidential Information for Appointments Form must be used in those circumstances where information is not identified in an electronic health system and it is not possible to identify the type of Confidential Information transported and/or the Client(s) or persons the information is about by other means.

- All Confidential Information (i.e. forms, schedules, labs, reports, etc.) must be securely fastened in a folder to ensure documents will not be separated, misplaced or lost.

- Where necessary, the sender shall enclose a copy of the tracking form with the information being transported.

- Confidential Information shall be:
  - Packaged and sealed prior to removal from originating site/program/office;
  - Transported with Southern Health-Santé Sud staff to ensure security at all times;
  - In a sealed envelope with sender's signature and current date written across the seal or in a locked briefcase or in a Confidential Information Security bag with the combination known only to sending and receiving parties; and
  - Notify the recipient that the Confidential Information has been forwarded.

- Where the Recipient is not the Sender, the Recipient of Confidential Information must confirm receipt of Confidential Information (e.g. chart, file, documents) by telephone or

email. Discrepancies in the number of Records received or failed delivery of Records shall immediately be addressed with the Sender.

- The Recipient must document receipt of Record(s) when required to use Southern Health-Santé Sud ORG.1411.PL.404.FORM.01 Tracking of Confidential Information Worksheet or ORG.1411.PL.404.FORM.02 Tracking-Transport-Confidential Information for Appointments Form.

Managers/Supervisors

- Managers/supervisors shall ensure that all Staff are made aware of this policy.

- Managers/supervisors shall periodically audit the transportation practices of Staff to ensure procedures are followed to minimize the risk of a Privacy Breach.

- An occurrence report must be completed for all Privacy Breaches, or opportunities to improve the transporation practices of Staff, and brought to the attention of the Privacy Officer/Advisor for corrective action. A copy of the occurrence report msut be forwarded to the Privacy and Access Specialist.

- If Confidential Information is perishable in certain conditions, any Agent retained to transport or deliver any Confidential Information for the Trustee shall be advised in writing of any specific information regarding the perishability of the information and the conditions necessary for the safe transport of the Confidential Information. For example, any service contract for the transport or delivery of Confidential Information shall contain:
  - A provision advising the service provider of the requirements to safeguard the confidentiality of Confidential Information and to physically protect it from unintended destruction including any appropriate cautions as to the perishability of the particular media used for the Confidential Information in question;
  - An agreement by the service provider that it and its Staff or Agents shall protect the confidentiality, Security and physical integrity of Confidential Information.

Privacy and Access Specialist or Designate

- Conduct periodic audits of building Security with regard to potential for unauthorized access to Confidential Information.

- Ensure provision is made for Confidential Information to be stored in a Secured Place.

- Remain informed of all Digital Health processes and policies related to the security and protection of Confidential Information.

- Keep a database of Privacy Breaches including, but not limited to Security and provide a summary of all Privacy Breaches in a monthly report to leadership.

SUPPORTING DOCUMENTS

ORG.1411.PL.404.FORM.01 Tracking of Confidential Information Worksheet
ORG.1411.PL.404.FORM.02 Tracking-Transport-Confidential Information Records for Appointments Form
ORG.1411.PL.404.FORM.03 Confidential Information Label

REFERENCES:

The Privacy Act
The Personal Health Information Act
The Freedom of Information and Protection of Privacy Act
WRHA *Confidentiality of Personal Health Information*, Policy #10.40.120.
ORG.1410.SG.001 Encrypting Records using 7-Zip File Manager
ORG.1411.PL.001.SD.01 - FIPPA Definitions
ORG.1411.SG.001 - Emailing Confidential Information
ORG.1411.PL.407 - Transmission of Personal Health Information via Facsimile
ORG.1411.PL.502.FORM.03 - Record of Access/Disclosure/Release of Personal Health Information Form
ORG.1411.PL.502.FORM.04 - Record of Access/Disclosure/Release of Personal Health Information (Community) Form
ORG.1411.PL.502.FORM.05 - Record of Disclosure of Personal Health Information (Community) Form
ORG. 1411.PL.502.SD.01 - Personal Health Information Act (PHA) Definitions