



Team Name: Health Information Services  Team Lead: Regional Officer, Privacy & Access  Approved by: VP – Finance & Planning	Reference Number: ORG.1411.SG.001  Program Area: Health Information Services  Policy Section: Privacy and Access
Issue Date: September 4, 2020 Review Date:  Revision Date:	Subject: Emailing Confidential Information

*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:**

Emailing Confidential Information

**PURPOSE:**

To protect personal health information and personal information under *The Personal Health Information Act (PHIA)* and *The Freedom of Information and Protection of Privacy Act (FIPPA)*.

To implement procedures to prevent the interception of Confidential Information by unauthorized persons where the trustee/public body’s intent is to disclose Confidential Information electronically (i.e. email).

To establish reasonable safeguards to protect Confidential Information when considering communicating by email outside of Southern Health-Santé Sud’s network.

To outline the associated risks of using emailing to share Confidential Information.

**DEFINITIONS:**

**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 confidential nature.

**Distribution Lists:** A feature of email programs that allows users to maintain a list of email addresses and send messages to all of them at once.

**Encryption:** a method of converting data to a secure and unreadable format. An individual must have a “key” (e.g. a password) to unscramble the code to read the data.

**Implied Consent:** In all circumstances, the purpose of the Use and Disclosure would become reasonably obvious to the Individual the information is about (or another Person Permitted to Exercise the Rights of the Individual), and it is reasonable to expect that they would consent and the information is Used or Disclosed only for the purpose it was collected. Consent is not given directly by the Individual.

**Secure Managed Environment:** Provides authentication, privacy and data integrity during transport between two communicating computer applications. For example; Transport Layer Security (TLS), emailing within a regional network or “firewall”, portals etc.

**Virus or Malware:** Any program designed to copy itself into other programs often resulting in alteration/loss of data and/or the disabling of computers and networks.

#### **IMPORTANT POINTS TO CONSIDER:**

Transferring Confidential Information by email carries significant risks including, but are not limited to:

- Interception: Email shared by multiple individuals (i.e. family members) can result in the wrong recipient reading the message.
- Misdirection: Sending information to the wrong email address (i.e. clients may have similar names and autocomplete populates the incorrect address or the client may have changed their email address).
- Inference: The name and nature of sender and/or attached material may reveal Confidential Information about an individual.
- Alteration: The recipient of an email could edit or alter a health care provider’s response and forward the changed message to a third party.
- Loss of Confidentiality: Group emails do not protect the names and/or email addresses of other group members if the blind carbon copy field (bcc) is not used.
- Loss of Information: Opening an email and/or attachment with a virus may damage files resulting in loss of data and information.

Confidential information should not be sent outside a Secure Managed Environment where more secure methods of communication are available.

Exceptions may be made in the following circumstances:

- There is an immediate requirement that necessitates the need to send Confidential Information by email.
- The purpose is for scheduling appointments where the individual and health professional have agreed it is necessary to maintain the health of the individual.
- Email is the only reasonable way to communicate with clients who do not have access to, or who are unable to, use other telecommunication methods (i.e. phone, fax).

An individual's email address is Confidential Information and must be protected by using the bcc field when sending generic information (i.e. newsletters, vacant shifts) using a distribution list.

**PROCEDURE:**

As a rule, email is not considered a secure method of disclosing Confidential Information and should not be relied upon when more secure methods of communication are available. However, if email is the **only** available method of communication or the **only** way to send the information, adhere to the following:

1. Consider the sensitivity of the Confidential Information and limit the amount of information in the body of the email to the minimum amount necessary to accomplish the purpose.
2. If practical, remove all or limit personal identifiers (e.g. Mr. Will Smith, becomes Mr. S or WS).
3. Do not include identifiable information in the subject line of the email. Use a brief description about the purpose of the email using initials or abbreviations (i.e. Follow-up, Letter, Contact or N.H. Confirm Time).
4. If reasonable, encrypt and password protect records containing Confidential Information and send as attachments. If assistance is required, contact Information and Communication Technology (ICT).
5. Communicate passwords by phone or, when that is not a reasonable option, at minimum, in a separate email message.
6. Confirm the name and email of the intended recipient(s) in the "To" field. Use caution when using the auto-complete list that displays previously used addresses automatically. Consider sending a test email.
7. Before using email to communicate with patients or clients, you must send an email that includes the language located in the Email Acknowledgment and Agreement - ORG.1411.SG.001.SD.01. Document in the health record that consent has been received (consent is implied if the patient or client proceeds with sharing information electronically).
8. As the sender, include your name and contact information within the body of the email, and avoid information that may reveal Confidential Information about a recipient's specific care. (i.e. remove the term "Oncologist" from Jane Smith, MD, CCFP, FCFP, Oncologist).
9. Where possible, confirm delivery of the email with delivery receipt or follow-up phone call.
10. If, despite the above-mentioned measures, a message is sent to the wrong email address, immediately take steps to recall the message or to reach out to the recipient and request they delete the message from their inbox, delete box and deleted items recovery. Notify your supervisor, manager or site Privacy Officer and complete an Occurrence Report (ORG.1810.PL.001.FORM.01).
11. Print emails with clinically relevant information for inclusion in the health record of the individual the information is about.

### **EMAIL BEST PRACTICE:**

- **NEVER** email Confidential Information to a health care provider's personal email account (Yahoo, Google, iCloud).
- **NEVER** forward work email to a personal email account.
- **NEVER** use email distribution lists to email Confidential Information.
- **NEVER** store personal health information in an email folder that belongs in the health record of the client.
- **NEVER** respond to email threads containing Confidential Information where that information is not necessary to be sent repeatedly. Delete the thread and start a new message.

### **SUPPORTING DOCUMENT**

[ORG.1411.SG.001.SD.01](#) - Email Acknowledgment and Agreement

### **REFERENCES:**

[ORG.1810.PL.001.FORM.01](#) - Occurrence Report

Shared health Guideline: Emailing Personal Health Information

Office of the Information and Privacy Commissioner of Alberta – Advisory for Communicating with Patients Electronically

Manitoba Ombudsman Practice Note – Privacy Considerations when Emailing Personal and Personal Health Information

Shared Health Collaborative Tools Matrix (<https://sharedhealthmb.ca/files/covid-19-collaborative-tools-matrix.pdf>.)