# Saskatchewan Cancer Agency

| | | | |
|---|---|---|---|
| **DIVISION:** | Corporate Services | **POLICY #:** IM 0029 | |
| **DEPARTMENT:** | Information Management Services | **ISSUE DATE:** April 3, 2018 | |
| **CATEGORY:** | Security and Confidentiality | **REVISED DATE:** | |
| **POLICY TITLE:** | Secure Electronic Transmission of Confidential Information | | |

**Policy Statement**

Confidential information in the Saskatchewan Cancer Agency's ("Agency") custody and control shall only be electronically transmitted by the terms laid out in this policy and supporting procedures and guidelines.

**Purpose**

This policy defines the conditions by which confidential information in the custody and control of the Agency must be securely transmitted by electronic mediums.

**Application**

This policy applies to the electronic transmission of confidential information sent via email, fax, and texting. This policy does not apply to the electronic communication of personal and/or health information with patients. It also does not apply to the electronic transmission of data from any health sector applications (e.g. EMRs, Pharmaceutical Information System (PIP), eHR Viewer) or Agency approved electronic systems.

This policy is also subject to all Agency documentation, guidelines and consent forms governing restrictions, permissible use, distribution, storage and destruction of photography, videos or audio containing confidential information.

Compliance with this policy applies to all Agency employees, and is pursuant to all applicable laws. Agency employees are responsible and accountable for protecting the confidentiality, privacy, and security of Agency information at all times, and only use such information for its intended purpose.

**Authority**

SCA Executive Leadership Team

| | |
|---|---|
| Approved by: _____ Signature | Date: May 29/18 |

## Definitions

***Agency Employees*** means all personnel employed by the Agency who are entitled to remuneration for services performed for the Agency or who have access to personal information, personal health information or other Agency information. This also includes all volunteers, research staff, and individuals of contracted companies, observers and students working at the Agency.

***Approved Agency Devices*** means any Agency approved device (smartphones, tablets, etc.) as referenced in the *BYOD Policy* (IMS-0020), or any Agency provided device (smartphones, tablets, etc.) as referenced in the *Mobile Device Policy* (IMS-0005).

***The Cancer Agency Act*** means the Act respecting the provision of cancer control services for the province of Saskatchewan.

***Confidential Information*** means information that has been disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure without permission. Confidential information includes all information, records, documents, data and software (including passwords), Personal Information (PI) within the meaning of *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP) and Personal Health Information (PHI) within the meaning of *The Health Information Protection Act* (HIPA)[1]. This also includes Agency business information and identifiable information.

***De-Identified Information*** means information from which any information that may be reasonably be expected to identify an individual has been removed (e.g. name, phone number, address)

***The Health Information Protection Act*** **(HIPA)** means the Act respecting the collection, use and disclosure of personal health information, access to personal health information and the privacy of individuals with respect to personal health information (Saskatchewan)

***Identifiable Information*** means information that can be used on its own or with other information to identify or re-identify an individual in context.

***The Local Authority Freedom of Information/Protection of Privacy Act*** **(LAFOIP)** means the Act respecting a right of access to documents of local authorities and a right of privacy with respect to personal information held by local authorities (Saskatchewan)

***Personal Health Information (PHI)*** means personal health information about a person (whether living or deceased) in any form or medium, and includes:

a. information with respect to the physical or mental health of the individual;
b. information with respect to any health service provided to the individual;
c. information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
d. information that is collected:
   **i.** in the course of providing health services to the individual; or
   **ii.** incidentally to the provision of health services to the individual; or
e. registration information.

[1] Saskatchewan Justice, *Personal Information Contract Checklist*

***Personal Information (PI)*** means personal information about an identifiable individual that is recorded in any form or medium, and includes[2] :

- Information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
- Information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- Information that relates to health care that has been received by the individual or to the health history of the individual;
- Any identifying number, symbol or other particular assigned to the individual;
- The home or business address, home or business telephone number, fingerprints or blood type of the individual;
- The personal opinions or views of the individual except where they are about another individual;
- Correspondence sent to a local authority by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;
- The views or opinions of another individual with respect to the individual;
- Information that was obtained on a tax return or gathered for the purpose of collecting tax;
- Information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or
- The name of the individual where:
    - It appears with other personal information that relates to the individual; or
    - The disclosure of the name itself would reveal personal information about the individual.

***Privacy*** means the right of the individual to exercise a measure of control over his or her PI and PHI. It involves the decision of the individual about what PI and PHI will be disclosed and for what purposes.

***Record*** means information (within the context of LA FOIP) in any form and it includes information that is written, photographed, recorded or stored in any manner but does not include computer programs or other mechanism that produce records. [3] For HIPA, this would apply to information in any form or medium that contains personal health information held by the Agency.

***Secure Health Sector Network*** means the secure IT network of the Saskatchewan health sector partners - the Saskatchewan Health Authority, the Ministry of Health, the Agency, 3sHealth, the Health Quality Council and eHealth Saskatchewan.[4]

***Text Messaging (Texting)*** means the transmission of messages from one device (e.g. phone, tablet or computer) to another device. For the purpose of this definition and document, this includes SMS texts (short message service) sent over a cellular data network, iMessages (texts sent to and from iOS devices and Macs), and other messaging tools or applications (e.g. WhatsApp) outside the secure health sector network and not approved by the Agency.

.

[2] LA FOIP s. 23-1
[3] Government of Saskatchewan (Ministry of Government Relations) – *Records Retention and Disposal Guide (May 2016)*
[4] Applicable only to email transmissions involving health sector email addresses, not personal email addresses.

## General Principles

### 1.0 Email

Transmission of confidential information by email must be in accordance with HIPA, LA FOIP, *The Cancer Agency Act*, this policy, and other applicable Agency policies and procedures. Emails between Agency employees and other users within the secure health sector network are permitted under the following conditions:

- Agency email users have reviewed the "*Email Best Practices Guidelines Sheet*" within the HR-512 *Acceptable Use Policy*, and understand their restrictions and responsibilities as Agency employees. *(Appendix A)*
- Email transmission of confidential information by Agency employees must originate from an Agency email address. No personal email accounts may be used to transmit or receive confidential information originating from or pertaining to the business of the Agency or the care of its patients.
- Agency employees must send emails with confidential information to contacts within the secure health sector network (e.g. Physician emailing a picture of a rash or malignant tumor to Patient Information Services to be included on the patient's health record) in compliance with the "*Email Best Practices Guidelines*".
- Agency employees must follow Information Technology (IT) security processes before transmitting confidential information to an external email address outside the secure health sector network. Further information about how to password protect a document can be found by either contacting the eHealth Service Desk for assistance, or by accessing the following link.
- The email subject line may provide general detail regarding the purpose of the email, but must not disclose any confidential information. Confidential information shall be placed in the body of the email, or as part of an attachment.
- Agency email accounts may be used to transmit attachments and/or pictures of patient related medical conditions taken on approved Agency devices.
- Only the least amount of information necessary shall be transferred by email (e.g. patient initials and S/R number).
- All communication via email must have the confidentiality statement: *"This email (including attachments, if any) is intended for one or more specific recipients and is legally privileged. Any privilege that exists is not waived. If you are not the intended recipient(s), any redistribution or copying of this message is strictly prohibited. If you have received this message in error, please notify me immediately by return email and delete this email. Thank you."*[5]

[5] HR-512 Acceptable Use Policy

## 2.0 Faxing

**Always consider if there is a more secure way to forward the information to the recipient, and only use faxing to transmit PI and PHI when no other options are available** (i.e. there is an immediate time requirement such as an emergency that necessitates faxing the confidential information).[6]

Transmission of confidential information by fax must be in accordance with HIPA and/or LA FOIP, this policy, and other applicable Agency policies and procedures. Faxing of confidential information is permitted under the following conditions:

- Agency users have reviewed the "*Faxing Best Practices Guidelines Sheet*" *(Appendix B)* and understand their restrictions and responsibilities as Agency employees.
- Only the least amount of information necessary shall be transferred by fax.
- Always confirm the fax number before sending. This applies to pre-programmed numbers as well.
- Always use a fax cover sheet that identifies the sender, the contact information for the sender, the intended recipient, the recipient's contact information and the total number of pages sent.
- All communication via fax must have the confidentiality statement "*This fax is intended for one or more specific recipients and is legally privileged. Any privilege that exists is not waived. If you are not the intended recipient(s), any redistribution or copying of this fax is strictly prohibited. If you have received this fax in error, please notify me immediately. Thank you."*

## 3.0 Texting

- Agency users have reviewed the "*Texting Best Practices Guidelines Sheet*" *(Appendix C)* and understand their restrictions and responsibilities as Agency employees.
- Text messaging of any confidential information by Agency employees is not permitted regardless of the device unless the Agency employees use secure, encrypted messaging applications that have been approved by the Agency (e.g. Cisco Jabber) to send confidential information.[7]
- Text messaging of de-identified patient information may be allowed; however, this may only be done in an administrative capacity[8] and only if proper record management practices are applied (when applicable). For example, it would be acceptable to text "Your 3pm patient has arrived and is waiting in your office". It would not be acceptable to text "Mrs. Robertson is in Room 3 at the ABCC waiting on her MRI results". (See Appendix C)

[6] *Fax vs. E-mail – Weighing the Fax*, Saskatchewan Information and Privacy Commissioner's office, 2016, https://oipc.sk.ca/fax-vs-e-mail-weighing-the-fax/

[7] These approved applications run through the secure health network, and have the same record management, security and privacy requirements as email. The messages are electronically logged for audit purposes and subject to access/freedom of information requests.

[8] Within the context of this policy, the use of texting for administrative purposes is not a mandatory requirement and is subject to the discretion and/or approval of an employee's manager/supervisor.

## 4.0 Documenting Transmission of Records

If information being electronically sent is determined to be a business record or part of a patient record under LA FOIP and/or HIPA, this information must be documented, stored, managed, and disposed of as defined by legislation and internal policies, procedure and best practices.

Personal health information that would normally be included in the health record (if delivered by electronic transmission mediums) is to be included in the health record by either including a printout of the information (and associated attachments), patient pictures and/or transcribing the relevant information as a narrative summary/note into the health record. This would also apply to personal information in corporate email and records.

## 5.0 Information Sent to an Unintended Recipient (Breach)

If an Agency employee sends confidential information to an unintended recipient, the following steps must be taken:

- Contact your manager and/or privacy officer (when appropriate).
- Contact the unintended recipient(s) and ask that they delete or destroy the information immediately (including from their deleted email folder). Receive written confirmation back once this has been done.
- Immediately file an UOMS report, documenting the breach and the mitigation steps that have been taken at the time of the report.
- Review and follow the "*Privacy Breach Response Protocol*" document.

## 6.0 Related Policies and Documentation

- PRI-0100 Collection, Use and Disclosure of Personal/Health Information
- PRI-0207 Disclosure of Personal Health Information
- PRI-0700 Privacy Breaches
- PRI-0800 Protection of Personal/Health Information
- HR-501 Confidentiality Agreement
- HR-512 Email Acceptable Use Policy
- SS-202 Safe Work Practices Policy
- IMS- 0020 BYOD Policy
- IMS-0005 – Mobile Device Policy

## 7.0 References

- Alberta Health Services Policy – *Transmission of Information by Facsimile or Electronic Email* (January 2015) https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-transmission-information.pdf
- Alberta Health Services Procedure – *Emailing Personal Identifiable Health Information (July 2016)* https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-email-personal-id-health-info-pro-1113-01.pdf
- Alberta Health Services – *Emailing Personal Identifiable Health Information Leading Practice User Guide (August 2016)* https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-email-

personal-id-health-info-pro-leading-practice-user-guide.pdf
- Information and Privacy Commissioner of Ontario – *The Secure Transfer of Information* (August 2012) https://www.ipc.on.ca/wp-content/uploads/Resources/fact-18-e.pdf
- Saskatchewan Office of the Information and Privacy Commissioner - *Faxing Personal Information and Personal Health Information,* (March 2015) https://oipc.sk.ca/assets/faxing-pi-and-phi.pdf
- Saskatchewan Office of the Information and Privacy Commissioner – *Fax vs Email - Weighing the Fax* (November 2016) https://oipc.sk.ca/fax-vs-e-mail-weighing-the-fax/
- Information and Privacy Commissioner of Ontario – *Communicating Personal Health Information by Email* (September 2016) https://www.ipc.on.ca/wp-content/uploads/2016/09/Health-Fact-Sheet-Communicating-PHI-by-Email-FINAL.pdf
- Interior Health - *Emailing and Text Messaging – Information for Patients*, October 2013, https://www.interiorhealth.ca/YourCare/MAiD/Documents/807393-Email%20and%20Text.pdf
- Interior Health – *Email and Text Messaging Policy*, May 2016, https://www.interiorhealth.ca/AboutUs/Policies/Documents/Email%20and%20Text%20Messaging.pdf

# Appendix A:

## SCA Privacy, Security and Access Guidelines
### Emailing Sensitive and Confidential Information (Secure Health Sector Network)

**PURPOSE:** The purpose of this document is to provide guidance to Saskatchewan Cancer Agency (Agency) personnel in respect to the email transmission of personal health information, personal information or any other sensitive information (confidential information).

**The guidelines below should be followed when sending emails to recipients within the secure health sector network:**

- Consider whether it is necessary to send any confidential information via email in order to carry out the task. Do not include unless it is absolutely required.
- Always try to send de-identified information whenever possible.
    - If you must provide a personal identifier, use initials, R/S number or health card numbers rather than names to anonymize the data.
    - Try not to have multiple personal identifiers in the same email.
- Do not have confidential information in the subject line.
- Use password protections (whenever reasonable to do so). This is recommended for external stakeholders, extremely sensitive information, or for large numbers of patients.
- Always ensure only the least of amount of information is provided to accomplish your purpose (data minimization rules). For example, do not sent a screenshot of a complete patient profile when only the HSN is required to fulfill the purpose or solve the issue.
- Ensure there is an Agency approved confidentiality notice in the email: *"This email (including attachments, if any) is intended for one or more specific recipients and is legally privileged. Any privilege that exists is not waived. If you are not the intended recipient(s), any redistribution or copying of this message is strictly prohibited. If you have received this message in error, please notify me immediately by return email and delete this email. Thank you."*[9]
- Always send and receive confidential Agency information from an authorized work email account (never from personal accounts).
- Confirm that the recipient email is up to date, and that you have selected the right email.
- Regularly check preprogrammed distribution lists to ensure they are up-to-date.
- Do not send any identifiable or confidential information to "group email" accounts, such as the "eHS Service Desk". These accounts tend to have multiple people who access the inbox, and are outside the "need to know".

**This guideline should be followed when emailing outside the secure health sector network:**

- No confidential information may be emailed outside the secure health network unless the communication is password protected. Passwords must be given to the recipients in a separate correspondence.[10]

**If you receive an email with confidential information in error, do not distribute it and notify the sender immediately. Consult your manager and/or the privacy officer when appropriate.**

**REFERENCES:**

- Information Management Handbook, Saskatchewan Ministry of Justice, http://publications.gov.sk.ca/documents/9/39676-InformationManagementHandbook.pdf
- Fax vs Email – Weighing the Fax!: https://oipc.sk.ca/fax-vs-e-mail-weighing-the-fax/
- Communicating Personal Health Information by Email: Information and Privacy Commissioner of Ontario - https://www.ipc.on.ca/wp-content/uploads/2016/09/Health-Fact-Sheet-Communicating-PHI-by-Email-FINAL.pdf

[9] HR-512 Acceptable Use Policy
[10] Emailing Agency patients/clients falls outside the scope of this document.

# Appendix B:

## SCA Privacy, Security and Access Guidelines
### Faxing Sensitive and Confidential Information

**Always consider if there is a more secure way to forward the information to the recipient, and only use faxing to transmit PI and Phi when no other options are available** (i.e. there is an immediate time requirement such as an emergency that necessitates faxing the confidential information).

**PURPOSE:** The purpose of this document is to provide guidance to Saskatchewan Cancer Agency (Agency) personnel in respect to the facsimile (fax) transmission of personal health information, personal information or any other sensitive information (confidential information) to and from the Agency.

**The following guidelines must be considered when faxing confidential information to and from the Agency:**

- Always use an Agency cover sheet that clearly lists the intended receiver, number of pages, your contact information and if the fax is confidential.
- Ensure there is an Agency approved confidentiality notice on the cover sheet that includes instructions on what to do if a fax is received in error.
  - "*This fax is intended for one or more specific recipients and is legally privileged. Any privilege that exists is not waived. If you are not the intended recipient(s), any redistribution or copying of this fax is strictly prohibited. If you have received this fax in error, please notify me immediately.*"
- Do not have identifiable, confidential or patient information on the cover sheet.
- Always try to send de-identified information whenever possible.
  - If you must provide a personal identifier, use initials, R/S number or health card numbers rather than names to anonymize the data.
- Always ensure only the least of amount of information is provided to accomplish your purpose (data minimization rules). For example, do not send a complete patient list when only one line is required.
- Always verify the fax number(s) before sending. Regularly check preprogrammed fax numbers/distribution lists to ensure they are up-to-date.
- Confirm if the fax is going to private or public fax line. For public fax lines, confirm time of transmission with the receiver.
- For received faxes, do not leave them sitting out and pick them up as soon as possible.
- Pre-program frequently used fax numbers. Update numbers as soon as you are notified of any changes or deletions.
- If you mistakenly send a fax to the wrong recipient, notify them promptly and request they destroy the fax in a secure manner or return to you. File an UOMS report regarding the incident. Work with your manager and Privacy Officer to ensure proper incident management steps are taken.

**If you receive in error a misdirected fax with confidential information notify the sender immediately. Consult your manager and/or the privacy officer when appropriate.**

**REFERENCES:**

- Faxing personal information and personal health Information: https://oipc.sk.ca/assets/faxing-pi-and-phi.pdf
- Use of Fax by Physicians: https://www.doctorsofbc.ca/sites/default/files/use_of_fax_by_physicians.pdf
- 10 Ways physicians can prevent privacy breaches when using fax: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2014/10-ways-physicians-can-prevent-privacy-breaches-when-using-fax-with-other-healthcare-professionals
- Faxing Personal Information: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/02_05_d_04/

# Appendix C:

## SCA Privacy, Security and Access Guidelines
### Considerations for Texting

**PURPOSE:** The purpose of this document is to provide guidance to Agency personnel on the use of short message service (text messaging) within their job roles for personal and Agency approved devices.

Texting can be a quick and effective way to communicate, but is not the ideal form of communication in the healthcare setting. For example, texting does not verify that the message has not been altered, or that it was successfully delivered to the end user's device. This leaves users vulnerable to sending messages that contain information that can be easily intercepted, read by and forwarded to anyone. Such messages are unencrypted and may be stored on the servers of telecommunication providers for significant periods of time.

**The following guidelines must be considered when using text messaging as a communication medium at the Agency:**

- Always consider when a face-to-face communication, email or phone call may be more appropriate.
- Under no circumstances will identifiable confidential information of the Agency be communicated via text messaging unless through secure, encrypted messaging applications that have been approved by the Agency. This includes de-identified information that, when linked with other data, may become identifiable back to an individual level.
- De-identify personal and personal health information sent by text messaging.
    - Rather than using a full patient/client name, use initials or the S/R number.
    - Do not text patient demographic or clinical information unless it has been de-identified.
- Limit or exclude individual identifiers when sending a text message.
- Consult with your manager to ensure that text messaging is an approved communication medium to support your specific job roles and responsibilities at the Agency.
- Take caution to ensure the correct contact/number is selected when texting.
- Only send the minimum information for the required purposes within the need to know.
- If something needs to be discussed that is time or content sensitive, request a meeting or arrange a telephone call**.** Do not rely on texting for these purposes.
- Do not use unacceptable abbreviations, internet slang, emotions, CAPITALS, **Bold**, etc.
- If any content of a text is considered part of the individual's record, ensure proper record management requirements are followed.
- If you receive a text message with personal health information in it, remember to apply record management principles - document appropriate clinical details and delete it from your device.

**Never respond to a text message that contains identifiable confidential information. Instead, send a new text message instructing the sender to call you directly. Consult with your manager and/or the privacy officer when appropriate. Delete the text once the sender is notified.**

**REFERENCES:**


- *Email and Text Messaging (AR0500)*, Interior Health https://www.interiorhealth.ca/AboutUs/Policies/Documents/Email%20and%20Text%20Messaging.pdf
- *Policy Statement: Texting in Health Care*, 2017, Healthcare Information and Management Systems society, http://www.himss.org/library/policy-statement-texting-health-care
- *Texting Policy*, 2016, Vancouver Coastal, http://medicalstaff.vch.ca/wp-content/uploads/sites/13/2016/03/texting.pdf
- *E-Communication: Communicating with Colleagues electronically*, 2018, CMPA, https://www.cmpa-acpm.ca/serve/docs/ela/goodpracticesguide/pages/communication/Privacy_and_Confidentiality/ecommunication-e.html