# Privacy, Security and Access to Personal Health Information

***Employee Learning Package***

www.saskcancer.ca

May 2018

# Table of Contents




# The Health Information Protection Act (HIPA)

## 1.1 What is HIPA?

*The Health Information Protection Act* (HIPA) is a provincial law that came into force on September 1, 2003. HIPA sets out rules and responsibilities for "trustees" (e.g. Cancer Agency employees, volunteers, contractors and physicians) who collect, store, use and disclose personal health information (PHI). It outlines an individual's rights in regard to protecting the privacy of and accessing their personal health information (PHI) that is held by a trustee.

## 1.2 Goal of HIPA

The goal of HIPA is to provide individuals with increased protection of their PHI, while at the same time ensuring that information is available on a **need-to-know basis** between health care providers to provide health services to the individual.

## 1.3 What is the definition of need-to-know?

There is no legal, medical definition in Saskatchewan for "circle of care", so we are moving away from using the phrase to support viewing, disclosing, or using PHI. The focus should be on the instance of care to define the need-to-know principle. The circle of care is very fluid to allow for possible involvement whereas the need to know is limited to those actually involved. Circle of care and need-to-know are much like football.

As with a football team, there are many different areas of expertise in a healthcare system. There are various squads that make up a team and the squads do not play all at once - in healthcare, not everyone is involved with an instance of care to an individual. Once an individual leaves a unit, then those in that unit are no longer in the instance of care and are outside the need to know.

**Consider this NEED TO KNOW check:**

- *Who needs to know?* **Individuals currently providing health services.**
- *Why do they need to know?* **Information is required to support or provide health services**.
- *What do they need to know?* **Only the minimum information required to provide the service.**

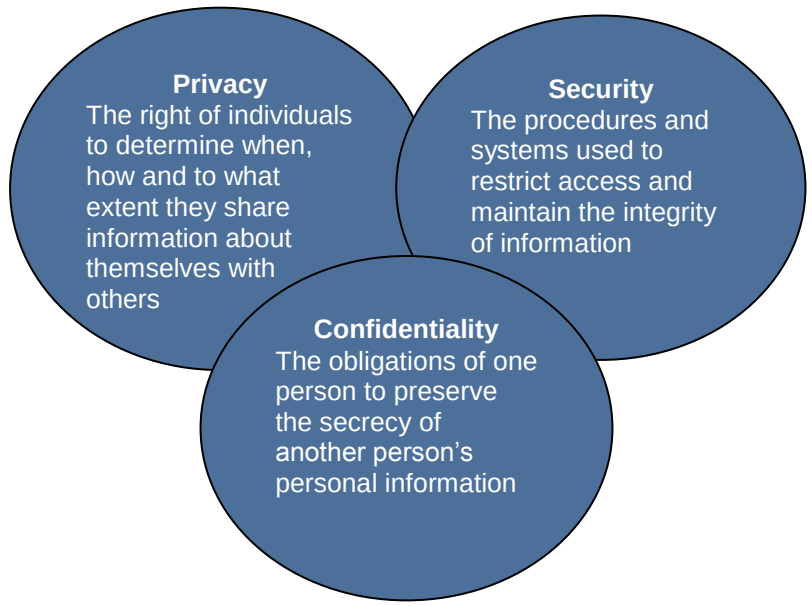
## 1.4 What is the definition of PHI?

PHI of an individual (whether living or deceased) is:

(i) information about an individual's physical or mental health;
(ii) information about any health service provided to the individual;
(iii) information about the individual's donation of body parts or bodily substances, or information obtained from the testing or examination of a body part or bodily substance of the individual;
(iv) information collected either in the course of providing health services to the individual, or incidentally to the provision of health services to the individual; or
(v) registration information (e.g. name, address, phone number, health services number)

### 1.5 Components Required to Protect Personal Health Information (PHI)

HIPA has three components required to protect PHI - privacy, confidentiality, and security. All three components are integral to the protection of PHI.




Privacy can be described as an individual's right to control the collection, use and disclosure of any information that relates to him or her.

The term confidentiality refers to the duty that we all have to protect information that has been entrusted to the Cancer Agency.

Security of information is about the controls that Cancer Agency has implemented to safeguard PHI from unauthorized viewing, use or disclosure and maintaining the integrity of the information.

The Cancer Agency has policies and procedures that detail appropriate viewing, collection, use, disclosure and storage of PHI.

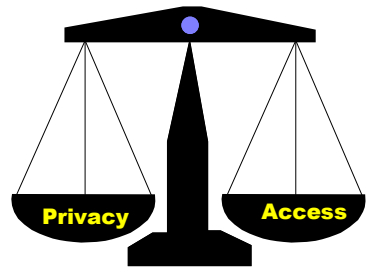
### 1.6 Who is a Trustee?

A trustee is a person or organization entrusted the custody and control of PHI. This means that we as employees and our employer, the Cancer Agency, have responsibilities under HIPA. There are many institutions, organizations, and individuals that qualify as trustees and are listed in section 2(t) of HIPA. Examples of trustees include: the Saskatchewan Health Authority, family physicians, dentists, private health professionals, and the Ministry of Health.

| REMEMBER: |
| --- |
| You signed a Confidentiality Agreement to respect the privacy of others, and you are bound by the principles and terms of that confidentiality agreement. What you learn at work is private and confidential. If it feels like gossip, it probably is. |

### 1.7 Trustee Responsibilities

HIPA lays out responsibilities for the trustee. The trustee must balance privacy (protecting the information) with rights of the individual (access to the information).




As a trustee, the Cancer Agency must have safeguards in place that protect the information, ensure appropriate viewing, use, disclosure, retention, storage, and disposal of PHI. Safeguards are defined by three main categories:

- Administrative- examples include: Data sharing agreements, privacy impact assessments (PIAs), confidentiality agreements, records management, and Cancer Agency policies and complementary procedures.
- Physical- examples include: locking doors and file cabinets, facility access controls such as restricted areas and design, and security personnel.
- Technical- examples include: firewall around the Cancer Agency computer network, controlled system user rights, database audits, individual user passwords, identification badges, video/closed circuit cameras.

As a trustee, the Cancer Agency must also comply with the “rights of the individual” outlined in HIPA.

### 1.8 Rights of the Individual

There are a number of rights of the individual prescribed in Part II of HIPA.

**An individual has the right to**:

- **consent** to the use and disclosure of his or her PHI;
- **revoke consent** to the collection, use, or disclosure of his or her PHI;
- **access** at any time his or her PHI or the PHI of a ward or child;
- be **informed** about how his or her PHI will be collected, used, and disclosed;
- request **amendment** of his or her PHI if there is an error or omission; and
- request a **review** by the Saskatchewan Information and Privacy Commissioner of actions or decisions of a trustee;
- refuse to disclose his or her health services number for services **other than** health services; and
- **designate**, in writing, another person to exercise individual rights on the person’s behalf.

## 2.0 Collection of PHI

The primary purpose for collecting PHI must be for the benefit of the individual according to section 24 of HIPA. Collect only what is needed to provide the health service to the individual. Collect the information directly from the individual, whenever possible. If this is not possible, note the person from whom you collected the information.

## 2.1 Use of PHI

HIPA states in section 26 that PHI must be used for the purposes it was collected and for a purpose that must primarily benefit the individual unless the individual has consented to use it for other purposes.

## 2.2 Disclosure of PHI

According to section 27 of HIPA, an individual is **deemed** to consent to the sharing of his or her PHI where the information is used and shared for the purpose of providing health care services to that individual. Therefore, deemed consent can be relied upon to use and share an individual's PHI on a **need-to-know basis** as required between health care practitioners to provide a health service to the individual rather than having to obtain express consent first. It is important to ensure that the health care practitioner is providing a health service to the individual.

Section 27 of HIPA also allows for Cancer Agency to rely on **deemed** consent to disclose an individual's PHI to family and close friends as long as the information disclosed relates to the health services currently being provided and the individual has not asked for privacy or that certain people not be advised.

There are numerous exceptions to relying on deemed consent to disclose an individual's PHI. Common exceptions include the following:

1) **To minimize a danger to the health or safety of any person:** "*Safety always overrides privacy*". This exception is not to be abused or taken lightly. There must be a legitimate and reasonable concern that someone's physical and mental safety is at risk. It is important to document on the individual's file, specifics of the dangerous situation, the date, time, details of information released and to whom it was released. It would be best practice to consult the Cancer Agency Privacy Officer on these decisions.

   HIPA protects the privacy of an individual's health information but is balanced to ensure that appropriate uses and disclosures of the information still may be made when necessary to treat a patient, to protect the public health, and for other critical purposes, such as when a provider seeks to warn or report that persons may be at risk of harm because of an individual. When a health care provider believes in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the individual or others, HIPA allows the provider, consistent with applicable law and standards of ethical conduct, to alert those persons whom the provider believes are reasonably able to prevent or lessen the threat.

Further, the provider is presumed to have had a good faith belief when his or her belief is based upon the provider's actual knowledge (i.e., based on the provider's own interaction with the individual) or in reliance on a credible representation by a person with apparent knowledge or authority (i.e., based on a credible report from a family member of the individual or other person).

The following logic test must be met prior to relying on this exception:

- There is a clear risk to an identifiable person or group of persons; and
- The risk is of serious bodily harm or death; and
- The danger is imminent; and
- The disclosure will eliminate or significantly reduce the risk.

2) **Where legally required to disclose PHI:** If a lawyer or police officer presents the Cancer Agency with a production order, warrant or subpoena requiring the disclosure of PHI, contact your area manager and the Privacy Officer immediately.

   Without a production order or subpoena, the Cancer Agency is limited to releasing to the police service the name, address, date of birth and telephone number of the individual, date and time of attendance and the nature and severity of the injury if it is proven that the disclosure will assist in enforcing or carrying out a lawful investigation pursuant to *The Criminal Code* or the *Controlled Drugs and Substances Act* (Canada).

   Gunshots and stab wounds receiving care in a "facility or hospital" are released to police officers under *The Gunshot and Stab Wounds Mandatory Reporting Act* and are limited to the type of wound, the individual's name if known and the location of the hospital or facility.

3) Where the disclosure is being made to obtain payment for the provision of a service to the individual.

4) Numerous other legislative Acts (or portions of such Acts) supersede the use and disclosure sections of HIPA. For example:
   a) *The Adoption Act*
   b) *The Automobile Accident Insurance Act*
   c) *The Child and Family Services Act*
   d) *The Public Disclosure Act*
   e) *The Public Health Act, 1994*
   f) *The Vital Statistics Act*
   g) *The Worker's Compensation Act*

**Check with your Manager**

Many of these Acts make it mandatory for the Cancer Agency to disclose certain PHI. Discuss with your manager or supervisor specifics on any of these Acts and how they may impact your area of work.

### 2.3 Individuals Requesting Access to their PHI

Individuals have a legal right at any time to see or obtain copies of their PHI. Individuals should be referred to the Cancer Agency Patient Information Services Department (PIS) for any access requests regarding their information and files.

**30 Day Time Limit**

Trustees must respond to a request for access to PHI within 30 calendar days of receipt of the request. There are provisions for a time extension under certain conditions; however, before an extension is sought, all efforts should be made to respond to the individual's request within the legislated time.

### 2.4 Amendment of PHI

If an individual reviews his or her file or obtains a copy and finds that it contains factual errors or omissions, he or she has a right to request a change or correction. Opinions are not subject to change or removal. This request must be made by the individual in writing. There is no specific form to use.

The Cancer Agency can either make the change if it agrees that there is a factual error or omission, or add an addendum to the record, noting that a difference of opinion exists and the record remains unchanged.

### 2.5 Review and Appeal

If an individual is unhappy with the Cancer Agency or any trustee in regards to something the trustee has done with his or her PHI, there is a provision within HIPA to assist in resolving the issue. The Information and Privacy Commissioner (IPC) of Saskatchewan, an independent officer of the Legislative Assembly, is available to review concerns by individuals in the following situations:

a) if the individual is not satisfied with a decision made by a trustee regarding access to his or her PHI;
b) if an individual believes that the request for correction or change to his or her PHI has not been made in accordance with HIPA;
c) if it is believed that HIPA has been disregarded (breached); or
d) if an individual believe that a fee charged by a trustee for access to PHI will cause undue hardship.

The powers of the Saskatchewan IPC are limited to an ombudsman role; however the Cancer Agency works to meet the standards set by its office. The IPC cannot order the trustee to do or not do something, but his/her office can review the situation based on HIPA legislation and then set down recommendations.

If the Cancer Agency chooses not to implement all the recommendations, the individual can proceed to an appeal process through the court system.

| Refer Privacy Complaints to the Privacy Officer |
| --- |
| If an individual expresses a concern in regards to how his or her PHI has been used or disclosed or with respect to an inability to access information, please ask that he or she contact the Cancer Agency Privacy Officer. This gives the Cancer Agency the opportunity to address the concern and assist in its resolution. The individual can still opt for a review by the IPC's office if the concern is not addressed to his or her satisfaction by the Privacy Officer. |

### 2.6 Offences

Since HIPA is a provincial law, there are potential consequences if it is not followed.

Individuals found guilty of an offence can receive a fine of up to $50,000.00, be imprisoned for up to one year, or both. This applies to Cancer Agency employees.

Corporations found guilty of an offence can be fined up to $500,000.00 per offence.

If there is a breach of HIPA within the Cancer Agency, the Privacy Officer undertakes an internal investigation to determine the severity of the breach, whether it was intentional or not, and who else should be involved in the investigation.

### 2.7 Consents

There are two things you should know about HIPA and consents.

1. Within HIPA legislation it does not state that consent must be in writing. What it does state is that the consent must be "expressed". Therefore either written or oral consent is acceptable. In some departments and situations, written consent is mandatory. If an oral consent is provided, ensure that you validate the individual's identity and then notate in the individual's file the specifics of the consent provided.

2. Consents under HIPA use "age of discernment" versus "age of majority". If an individual under 18 years of age wishes to deny access to his or her PHI to a parent, the health professional must first determine whether he or she have the maturity level to make the decision and that

he or she understands the consequences associated with the decision. If the health professional assesses that the mature level is make decisions, then the Cancer Agency must comply with the individual's wishes.

### 2.8 12 Simple Things You Can Do

All that the Cancer Agency asks of employees is to: **Do the best that you can do to contain personal health information.** There are 12 simple things that are within your power to control and that you can do to respect privacy and confidentiality:

| **Self Look-up in Electronic Systems is Strictly Prohibited:** |
|---|
| If you want access to your information in Cancer Agency systems, please contact Patient Information Services. If you want copies of or access to your PHI such as lab results, radiology reports, chronic disease management reports and/or discharge summaries in provincial electronic systems, contact eHealth Saskatchewan at: https://www.ehealthsask.ca/Documents/Privacy%20and%20Access/eHS%20Request%20for%20Access%20to%20PHI%20Form.pdf |

1. There are many things that an employee does not have control over and one is how Cancer Agency facilities are designed. Currently, the design in many work areas does not enhance confidentiality and privacy (e.g. curtains instead of acoustical barriers between individuals who are receiving care). PHI should **never** be discussed:
    a) in public areas within the Cancer Agency facilities (e.g., elevators, hallways, washrooms, cafeterias);
    b) at home;
    c) in public areas outside Cancer Agency (e.g. restaurants, coffee shops)

    Privacy is very unique to each person. One person tell his or her whole life story without prompting - the good, the bad, and the ugly. Another person will not share anything with anyone unless there is a reason and/or there is trust the person will keep the information confidential. Respect each individual's unique perspective on privacy.

    A common question asked is "if you don't use the individual's name, is that enough to ensure individual anonymity and not be considered a HIPA breach?" The answer is unequivocally, "**NO".** De-identified PHI (which is not protected by HIPA) is defined as PHI from which any information that may reasonably be expected to identify an individual has been removed. In some cases, it could be easy to identify the individual, even without using the individual's name. Therefore, simply removing the individual's name may not be sufficient to de-identify the PHI, and disclosing same would contravene the requirements of HIPA.

2. Never share your computer password. Remember to change your password regularly or if you suspect someone has found out your password. Each person using the Cancer Agency information system has been given user rights based on specific job requirements. If someone enters the system using your password and does something inappropriate in the system, you are responsible. Compare this situation to the photo radar at the traffic lights. If your vehicle goes through a red light, you get the ticket even if you are not driving because the car is licensed in your name.

3. When away from your computer, always log off or lock your work station using the Ctrl+Alt+Delete function.

4. Turn the computer screen away from those that do not need to see the information or use a privacy screen so those around your computer cannot see what is on the screen.

5. View or use patient information on a need to know basis only. HIPA is all about need to know, not nice to know. Cancer Agency employees have broad user rights to information systems. We can view many individual files, including individuals that we are not looking after. Viewing

information on family, friends, and neighbours through the information system is not appropriate. Sometimes a person may use the information system for what may feel like a good reason such as finding out a colleague's birth date to celebrate the occasion. **This is a privacy breach in HIPA**. Instead, telephone a spouse or family member to find out the information. Another example is using the information system to find out if a friend or colleague is ill and what the type of illness. **This is a privacy breach in HIPA**. Call the family and find out the information.

6. Place fax machines in secure areas. Fax machines that are used to transmit PHI must be placed in an area that does not allow the public or other employees who do not have a need to know to view the information. Refer to the faxing guidelines on Page 10 when sending a fax containing confidential information.

7. Dispose of paper containing PHI in a locked confidential shredding bin or use a cross-cut shredder in your area. Remember cheat sheets and quick notes that you make throughout your day since they will likely contain PHI. Do not put paper containing PHI in regular garbage cans or recycle bins.

9. Lock file cabinets, desk drawers, offices, and storage areas containing PHI to reduce the risk of unauthorized personnel coming into contact with the information. Determine what amount of risk you or your department is willing to accept, and establish mitigation rules. Some areas within the Cancer Agency lock office doors (1 level of security) while other areas lock office doors and file cabinets (2 levels of security).

10. Practice the clean confidential desk principle. Remove confidential information or PHI from your desk when you are not in attendance. Tuck it away in a desk drawer or file cabinet. *Out of sight - Out of mind*. It helps reduce the temptation of people "sneaking a peek".

11. Speak with your manager or supervisor about any questions or concerns. The Cancer Agency Privacy Officer or security unit may be of assistance if your manager or supervisor is unavailable.

### 2.9 Resources/Contacts for Questions or Concerns

We know that, following this program, you may have additional questions or concerns. Here are a number of resources or contacts that may be of assistance to you:

- Supervisor or manager should always be the first line of contact
- Privacy Officer – Karen McAuley, you can email her at privacy@saskcancer.ca
- Saskatchewan Information and Privacy Commissioner- Ron Kruzenski, Q.C. - www.oipc.sk.ca or via email at webmaster@oipc.sk.ca
- There are HIPA specific policies, procedures and guidelines for privacy and security located on the Cancer Agency intranet site.

If you're not sure what you should do when PHI is requested, do not share the information. Ask someone who might know the answer (e.g. supervisor, manager, Privacy Officer).

If you think you have knowledge of a privacy breach or an inappropriate practice, please contact your manager or the Privacy Officer. Your concern can be made anonymously.

| This Package is based upon: |
| --- |
| *Let's Talk About HIPA – RQHR's on-Line Learning Package*", 2017 |

# 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."*[1]
- 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.[2]

**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


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

# 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/

## 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