eCOMMUNICATION

Considerations for trustees to protect personal health information when using eCommunication

This document is intended to provide general advice to trustees on how to protect personal health information when using eCommunication.

April 2019

Office of the
Saskatchewan Information
and Privacy Commissioner

eCOMMUNICATION

BACKGROUND

eCommunication, or electronic communication, is a continuously growing method of communicating between individuals. In healthcare, eCommunications tools are emerging to assist trustees in managing patients' healthcare by communicating directly with patients and other healthcare providers. Some eCommunication tools that are being utilized by trustees include email, text and picture messaging, video conferencing, mobile applications (apps), social media and patient portals. The tools used for eCommunication will continue to grow as technology advances and other forms of electronic communication are developed. This resource will discuss considerations for trustees when communicating personal health information (PHI) through eCommunications. For guidance on the management of text messaging and other instant messaging tools and tips for securing your mobile device, please refer to our resource: *Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools* and *Helpful Tips: Mobile Device Security*.

This document will provide trustees with considerations when using eCommunication to assist them in complying with their obligation under *The Health Information Protection Act* (HIPA). For HIPA to apply, there must be three elements present: 1) a trustee as defined at subsection 2(t) of HIPA; 2) there must be PHI; and 3) the trustee must have custody or control of the PHI. For further clarification on when HIPA is engaged and who is considered to be 'the trustee', please refer to the *IPC Guide to HIPA*.

There have been instances where our office finds that a healthcare provider, that fits the definition of a trustee, does not have custody or control of the PHI and thus, is not 'the trustee' of the PHI. An example of this can be found in Investigation Report 022-2018. In that report, the Commissioner found that the non-profit corporation that owned the medical clinic had custody and control of PHI, not the physicians of the medical clinic. In that case, as the non-profit corporation did not fit the definition of a trustee pursuant to HIPA, it was unfortunately found that HIPA did not apply. However, it is best practice that anyone that has custody or control of PHI appropriately protect PHI, including when they are using eCommunication.

PRIOR TO USING ECOMMUNICATION TOOLS, TRUSTEES SHOULD DETERMINE IF IT IS NECESSARY

Prior to using eCommunication tools, trustees should conduct a privacy impact assessment (PIA) to assist them in determining whether the use of eCommunication tools would be secure, appropriate and necessary, and whether the benefits outweigh the risks. For more information about conducting PIA's, consult our resource: *Privacy Impact Assessment: A Guidance Document*.

Trustees are responsible for assessing the risks associated with utilizing eCommunication tools for communicating PHI. The risks associated with each eCommunication tool will vary based on trustee organizations, the actions the trustee intends to take with the PHI and what type of PHI will be communicated through the eCommunication tool. Some of the risks that trustees may face when utilizing eCommunication for communicating PHI include:

- PHI may be used and disclosed to unauthorized users;
- PHI may be sent to the correct addressee but a third party intercepts the information (spouse, child, friend, etc.);
- Malware, such as worms and Trojan viruses may compromise the integrity of PHI communicated through the eCommunication tool;
- Access to information may be more susceptible to inappropriate changes or modifications;
- Unintended recipients may receive PHI through misdirected eCommunications such as email, text or picture messaging, resulting in a breach of privacy;
- Third parties, such as app developers, may use the information stored on the eCommunication tool for unauthorized internal or external use;
- Mobile devices that are used to communicate PHI through the eCommunication tools may be lost or stolen;
- Information or images posted on social media may identify a patient, thus compromising their privacy of the patient's PHI;
- Information posted on social media and public forums may never be completely deleted from the internet;
- Unauthorized personnel may overhear a phone call or video conference regarding PHI;
- Photos taken with a mobile device that capture a patient's PHI sent through an eCommunication tool may be viewed by others without a need-to-know;
- PHI may be accessed intentionally, such as by hackers, even if a passcode is in place; and
- Unauthorized access to PHI may be done through unsecured and public networks.

WHAT OBLIGATIONS DO TRUSTEES HAVE UNDER HIPA REGARDING PROTECTION OF PERSONAL HEALTH INFORMATION WHEN UTILIZING ECOMMUNICATIONS?

The IPC strongly recommends that trustees and their employees refrain from using eCommunication tools unless they can be set up to retain and store records automatically. When considering the implementation of any new eCommunication tool, trustees should consult with its access and privacy staff, information technology staff and records management staff to discuss whether the use of the eCommunication tool is necessary and if so, how the trustee will ensure that PHI will be appropriately safeguarded.

HIPA and the *HIPA Regulations* provide rules regarding when a trustee may collect, use and disclose PHI. Section 23 of HIPA requires trustees to ensure the collection, use and disclosure of PHI is on a need-to-know basis. Trustees must establish policies and procedures to restrict access to PHI by their employees without a need-to-know. Any unauthorized collection, use, or disclosure of PHI would be considered a privacy breach.

Section 16 of HIPA requires that a trustee have administrative, technical and physical safeguards to protect the integrity, accuracy and confidentiality of PHI in its possession or under its control from:

- Any reasonably anticipated threat, hazard or loss;
- Unauthorized access to or use, disclose or modification; and
- Otherwise ensure compliance with HIPA by its employees.

Administrative safeguards

Administrative safeguards are controls that focus on internal organizations, policies, procedures and maintenance of security measures that protect PHI.

Examples of administrative safeguards for trustees to consider when implementing the use of eCommunication includes:

- **Policies and procedures:** Develop and implement strong and clear written policies and procedures for the use of eCommunication tools to protect PHI to ensure staff are aware of the policies and how to apply them in practice.

  Some topics that trustees should ensure the policies address include: identifying which eCommunication tools are permitted for communicating PHI; identifying what type of PHI can be communicated through eCommunication and for what purpose; ensure staff are aware that all PHI communicated through eCommunication tools are official records and must be considered when processing access to information requests; ensure staff are aware that to limit the PHI collected, used and disclosed through eCommunication to meet the data minimization principle; ensure procedures are in place for how to respond to a suspected privacy breach involving an eCommunication tool or a lost or stolen device that is used to communicate PHI through eCommunication tools; and ensure staff know steps to take in verifying the identify of individuals that they plan to communicate PHI with through eCommunication.

- **Consent Forms:** Section 6 of HIPA indicates that consent to the collection, use or disclosure of PHI is informed if the individual who gives consent is provided with the information that a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure of PHI. Trustees planning to gather consent from patients to communicate with them via eCommunication should clarify what information they intend to communicate through these tools and the risks associated with using eCommunication. Trustees and their staff should also know how to address patient's

consent directives (example: patient wishes to have appointment confirmation and reminders via eCommunication but does not wish for test results or follow up information regarding a diagnosis to be sent via eCommunication). For more information on gathering informed consent, please refer to our resource: *Best Practices for Gathering Informed Consent and the Content of Consent Forms*.

- **Confidentiality/Privacy Agreement:** Ensure the Confidentiality Agreement/Privacy Agreement signed by staff includes reference to the eCommunication tools utilized by the trustee and what the expectations are when communicating PHI. For more guidance on this topic, please refer to our resource: *Sample Privacy Agreement for Trustees: Protection of Personal Health Information*.

- **Annual Access and Privacy Training:** Trustees should provide staff with training on expectations to properly safeguard PHI when implementing the use of eCommunication tools. Mandatory annual access and privacy training should also address the expectations of using eCommunication.

- **Information management service provider (IMSP) Agreements:** Ensure that when engaging with IMSPs for eCommunication tools that detailed written agreements are in place. For guidance on what elements should be included in such agreements, refer to section 18 of the *IPC Guide to HIPA* and our resource: *Best Practices for Information Sharing Agreements*.

- **Auditing Programs:** Determine the frequency that access or audit logs will be conducted on the eCommunication tools and PHI collected, used or disclosed through them to record whom accessed, modified or deleted the PHI. For more information about audit logs, consult our resource: *Audit and Monitoring Guidelines for Trustees*.

- **Records and Information Management Systems:** Trustees should determine how information will be sent, received and captured using eCommunication and ensure that the records produced by all authorized eCommunication tools are included in the overarching records management plans.

- **Records Retention and Destruction Schedules:** Records created through all authorized eCommunication tools should be included in the trustee's retention schedules and general records management planning. Trustees should also determine proper disposal methods of PHI from a device utilizing eCommunication tools or PHI stored in an eCommunication tool once the PHI has been transferred to a secure location.

- **Access Restrictions:** Determine which employees of the trustee require access to the eCommunication tools to ensure compliance with the need-to-know principle and have

access privileges revoked when necessary (example: employee leave of absence or termination of employment).

Technical Safeguards are the technology and the policy and procedures for its use that protect PHI and control access to it.

Examples of technical safeguards for trustees to consider when implementing the use of eCommunication includes:

- **Login Credentials:** Ensure all users have separate user names and passwords for accessing eCommunication systems and requiring that password-enabled screen locks are engaged using a strong password for mobile devices or other computer devices that are used for eCommunication.

- **Authentication Controls:** Consider what type of file, program or data permissions will be used to limit users access to the eCommunication tools or the PHI collected, used or disclosed.

- **Software and Operating Systems:** Disable unauthorized software on work-issued mobile and other computing devices and identify when software and Operating Systems (OS) should be updated and the consequences if not done so in a timely manner.

- **Virus Protection:** Ensure appropriate level of virus protection on devices where eCommunication tools are utilized and limit the types of apps or internet use on devices where eCommunication will be used to communicate PHI to minimize the risk of viruses.

- **Audit Capabilities:** Ensure any systems used for eCommunication of PHI have appropriate audit capabilities to monitor and audit the collection, use, disclosure, modification of deletion of PHI.

- **Secure Transmission of Data:** Ensure PHI communicated through eCommunication is appropriately protected, such as through the use of encryption and/or password protection.

- **Backup and Secure Storage of PHI:** Trustees should ensure that PHI collected through eCommunication tools are regularly backed up. Trustees should also determine if records can be automatically and securely retained on the trustees digital storage or if Mobile Device Management (MDM) or if Private Cloud Computing infrastructures will be utilized. If utilizing Cloud Computing infrastructures, determine where records are stored (ex. will the information be stored on servers outside of Canada) and ensure that the trustee will have control over how that information is protected, disclosed or accessed. Trustees should ensure the use of personal cloud services and their associated automatic back-up options

(ex. OneDrive or Dropbox) are not used on the trustees devices where eCommunication tools will be used. For PHI stored in eCommunication systems, trustees should determine if the information is encrypted.

- **Format of electronic records:** When using eCommunicaiton tools it is likely all records associated will be stored in an electronic format. To ensure the accessibility and integrity of the records, trustees should determine if the format the records are saved in will require separate software, or how to convert the record into a format that will be in an accessible and stable format.

Physical Safeguards are physical measures, policies, and procedures to protect PHI and related buildings and equipment, from unauthorized intrusion and natural and environmental hazards.

Examples of physical safeguards for trustees to consider when implementing the use of eCommunication includes:

- **Locked storage cabinets and offices:** Determine how eCommunication devices will be secured and stored when not in use.

- **Transportation of mobile devices:** Trustees should determine if it is necessary for devices that utilized eCommunication tools to be removed from the office. Trustees should ensure that devices being used to communicate PHI through eCommunication are appropriately secured in transit or when being used outside of the office (examples: transport in a locked briefcase or use a laptop lock when being used outside of the office).

- **Clean Desk Policy:** While clean desk policies are more commonly considered for safeguarding paper records, clean desk policies can also be implemented by trustees to prevent devices that are utilized to communicate PHI through eCommunication tools from being easily accessible to unauthorized users. (Examples may be placing mobile devices (such as smart phones and tablets) in a locked desk while unattended and utilizing laptop locks)

Consult our resource *Helpful Tips: Mobile Device Security*, for more guidance on physical safeguards for mobile devices.

What eCommunication Tools are being utilized in the healthcare field and what are some considerations for trustees?

Telemedicine

Telemedicine is a combined term meaning the delivery of health services and the use of technology to do so. Telemedicine can also be referred to as telehealth, telehomecare, telepresence and

telesurgery. The delivery of telemedicine can be done through the use of video conferencing, email, text and picture messaging, the use of apps and social media and patient portals. Telemedicine provides a means of communication between a patient and their health care provider and can be used for a variety of reasons such as medical consultation and coaching for chronic diseases or clinical reasons such as downloading blood pressure readings.

Video Conferencing

Some considerations for trustees include:

- Conduct video conferences in a secure area for telemedicine programs to take place (ex. designated telehealth room, sound proof room) and ensure patients also have a secure area for the video conference;
- Physical safeguards (ex. equipment is in a locked and limited access room);
- Determine whether the telehealth video conferences are recorded and stored;
- If video conferences will be recorded, determine what length of time they will be stored and how to integrate into the patient's record; and
- Ensure video conferences are conducted over a secure network connection. Determine if the data transmission will be encrypted.

Email

Some considerations for trustees include:

- Ensuring all PHI is in an attached document and is protected with encryption or passwords;
- Consider de-identifying the PHI that will be communicated;
- Consider using a file-share service that restricts the users that can access the records and limits the amount of time the information is available to other parties;
- Consider whether it would be more appropriate to send an email notifying patients that new results or messages await in a patient portal;
- Ensure recipient email addresses are accurate and up-to-date; and
- Ensure that suspicious emails or email addresses are reported to Information Technology staff for clearance or to block future emails.

For more information on safeguarding PHI when using emails, refer to our blog: *Fax vs. Email – Weighing the* Fax. The blog will discuss how the safeguarding of PHI communicated by the two different technologies differ. Trustees utilizing fax to communicate PHI should also refer to our resource: *Faxing Personal Information and Personal Health Information: Safeguards and Responding to a Breach*.

Text and Picture Messaging

Some considerations for trustees include:

- Determine whether PHI communicated through Text and Picture Messaging is to be stored on the mobile device and how it will be integrated into the trustees records management system;
- Create policies and educate staff on acceptable and unacceptable uses of text and picture messaging;
- Determine what type of information can be communicated through text and picture messaging, such as whether it will be used solely for confirming or scheduling an appointment or if the trustee will use the eCommunication for other actions;
- Consider de-identifying the PHI and what will be communicated through text messaging; and
- Ensure recipient contact information is accurate and up-to-date.

Mobile Applications (Apps)

Mobile applications (apps) are software created to be used on mobile devices such as smart phones and tablets. The use of apps may provide an alternative method of communicating between trustees and patients. Some health care providers are turning to the use of apps to document a patient's PHI, order tests or as a medical reference (ex. medical dictionary). Some considerations for trustees include:

- Trustees allowing the use of apps on mobile devices should consider developing a list of approved apps that can be installed on mobile devices to ensure the protection of PHI;
- Ensuring developers will not be accessing or sharing information for internal or external use;
- Ensure safeguards are in place to protect PHI stored in the app from being accessed by other apps on a patient's mobile device; and
- Limit what information the app will need access to on the patient's device and ensure patients have the choice to opt-in to app permissions to share information.

For more tips on the use of apps, refer to the Office of the Privacy Commissioner of Canada's resources: *Ten Tips for Communicating Privacy Practices to Your App's Users* and *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*.

Social Media

The use of social media to exchange information and knowledge and for connecting the profession of medicine to the general public is developing at a rapid pace but have inherent risks. Trustees are using social media as a tool to provide indirect medical care, offer advice, promote good health and communicate with fellow health professionals. Common social media platforms are Facebook, Twitter, Instagram and even blogs. Some considerations for trustees include:

- Trustees should prohibit discussions with individuals regarding any specific concerns regarding their PHI in a public forum;
- Trustees should develop policies regarding the use of personal social media accounts by employees to ensure PHI is not shared through those accounts;
- If trustees are considering use of social media private messaging tools (such as Facebook messenger) they should determine how those records will be retained, and should consider limiting the type of information that can be discussed through those tools; and
- Ensure content and images being posted on social media have been reviewed for information that may identify an individual.

Patient Portal

The adoption of the patient portal is growing in the delivery of health care. The patient portal is a new development aimed at not only providing patient's online access to their PHI, but also providing patients with the ability to communicate with trustees through the addition of PHI to their record. Some consideration for trustees include:

- Limit the amount and type of information a patient may add to their portal to avoid over-collection of PHI;
- Determine if patients will be able to access the patient portal on a mobile or mobile computing device (ex. smartphone) or only on a desktop or laptop computer;
- Identify, if using mobile or computing devices, what information the patient portal may collect from the patients mobile device;
- Avoid storing sensitive information in the portal and determine if patients will have the option of masking or blocking information made available through the portal; and
- Determine what technical safeguards will be implemented to protect patients' PHI when they are accessing the portal through their personal devices (ex. Will the session timeout after a specified length of inactivity? What will the log-in requirements be for patients? Will there be notice that patients should refrain from accessing their PHI or saving log-in information for the portal on publicly accessible devices?).

CONCLUSION

The term eCommunication and the capabilities of eCommunication tools will continue to grow with the advancement of technology and in turn, the number of trustees that utilize these tools and the actions they take with these tools. However, trustees need to ensure they consider the risks associated with using eCommunication to communicate PHI and take steps to ensure the information is appropriately safeguarded in compliance with HIPA.

CONTACT INFORMATION

If you have any questions or concerns regarding eCommunication, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

webmaster@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC