Guidelines for Use of Email or Fax

This section will:

- summarize the benefits and privacy risks associated with the use of email or fax in the clinical context
- identify key considerations for physician's offices that use email or fax to transmit personal health information

Physicians must take steps to reduce the risks associated with email or fax communications and ensure that reasonable safeguards are in place to protect personal health information.

What are the risks?

When using email or fax to transmit personal health information to patients, the following issues may negatively impact patient care:

- difficulties:
    - confirming the identity of the patient in an incoming email or fax
    - ensuring the correct recipient with only the patient's name, email address or fax number, as patients may have similar names
- risk to patients:
    - suffering adverse health consequences if it is an urgent matter and there is a delay in the response time
    - misinterpreting the content of an email or fax, which could lead to:
        - adverse health consequences
        - a complaint
        - legal action if the patient's perception is one of inadequate or ineffective communication

Using email to communicate with patients or third party health providers can give rise to the following privacy and security issues.

- An email message that is not encrypted can be:
    - intercepted by unauthorized third parties
    - altered and forwarded to unintended recipients

- Email messages containing personal information can be intercepted by unauthorized third parties if the email is:
    - delivered to the wrong address;
    - sent or received from unsecured locations such as those publicly accessible or a shared home computer;
    - retained on a home computer;
    - sent or received using a public Wi-Fi network;
    - shared by internet service providers with other third parties; or
    - saved on unsecured backup servers and subject to improper organizational retention rules.
- Attachments in an email may contain viruses that could cause serious damage to computer systems.
- The personal health information being emailed may leave Canada during transmission, and may be subject to laws in other jurisdictions that have inadequate protections or no protections at all.
- Faxing personal health information can have privacy and security risks of personal information being accessed by unauthorized third parties if the fax is:
    - sent to an incorrect fax number (caused by misdialling or by pressing the wrong speed-dial key);
    - exposed to unauthorized individuals simply because the fax machine is located in an open, unsecured location; or
    - accessed by third parties who are tapping into or monitoring the transmission.

Best Practices

Consider informing patients:

- about how emailing or faxing personal information can result in accidental disclosure or interception by other people not intended to receive the information
- what precautions the practice has taken to reduce the risks
- if the personal information is very sensitive, what other delivery options exists that are more secure (e.g., photocopies sent by mail or courier)
- that they can withdraw consent at any time to using fax or email as a method of communication, and how to do so

Office policies on use of email and fax usually include:

- criteria for the patient-provider communication, acceptable use, email etiquette, and management of email documentation as part of the patient's medical record
- staff training on the

- appropriate use of email and fax
- maintenance of emailed or faxed documents

- a process to remove a patient from email or fax communications if the patient withdraws consent to using any of these methods of communication
- appropriate destruction methods for emails and faxes, including deletion of emails from computer hard drive and faxes from memory

When communicating with patients or third party health care providers by email:

- Only use email systems that encrypt the email transmission and incoming and outgoing emails (or that apply other similar industry-standard protections).
- Protect each email inbox that is used to send or receive messages with a secure password known only by the individuals authorized to access the inbox.
- Protect any attached documents with a strong password and call the recipient to let them know.
- Confirm that you have the correct email address for the intended recipient.
- Verify email addresses regularly as they can be duplicated, and may frequently change.
- Whenever possible, leave sensitive personal health information out of the email or use obscure identifiers to protect it during transmission (e.g., avoid disclosing a patient's prognosis or diagnosis in an email, and instead ask them to call and make an appointment with the physician to get their results).
- Add a confidentiality disclaimer to email messages that states
  - the content is confidential and only intended for the stated recipient
  - anyone receiving the email in error must notify the sender and return or destroy the email
- For sensitive personal health information, contact the recipient by phone to inform them that confidential information is being sent and ask the recipient to call back to confirm receipt.
- Never use email distribution lists to send personal health information.

When communicating with patients or third party health care providers by fax:

- Only use fax systems that encrypt the fax transmission and incoming and outgoing faxes (or that apply other similar industry-standard protections).
- Protect the fax machine or the fax modem (a fax device that uses a computer program) with a secure password known only by individuals in the office who are authorized to send or receive faxes.
- Ensure the fax machine is located in a secure area in your practice to prevent unauthorized persons from viewing or receiving the documents.

- Always use a fax cover sheet that identifies both the sender and recipient with contact information and states the total number of pages being sent.
- Whenever possible, leave sensitive personal information out of the fax or use obscure identifiers to protect it during transmission
- Include a disclaimer stating
    - the faxed material is confidential and only intended for the stated recipient
    - anyone receiving the fax in error must immediately notify the sender and return or destroy the fax
- Before faxing the information, confirm the recipient's fax number (including when using a pre-programmed number) and confirm that the personal health information will be protected upon receipt
- If using pre-programmed fax numbers, regularly verify these numbers for accuracy
- Check the fax confirmation report as soon as the fax has been sent to confirm that the fax went to the correct place and that all pages were transmitted and received
- Check each day's fax history report for errors or unauthorized faxing
- When receiving faxes
    - retrieve documents sent by fax as soon as they have been processed
    - do not leave the documents sitting on or near the fax machine
    - if a fax is received in error, promptly notify the sender and return or destroy the information

Sharing fax machines with other offices is discouraged, particularly where personal information is frequently sent and received.

Although PIPA does not require it, a best practice is to avoid the disclosure of personal health information outside of Canada and prohibit access to such records from outside Canada without express patient consent.

Retention of Emails or Fax Documents

For storage and retention of emails and faxes, consider the following:

- Do not make or retain more copies of email communications than needed.
- Securely destroy extra copies that are no longer needed.
- Include personal health information that is emailed as part of the patient's medical record.

For additional information on emailing personal health information, see Emailing Patient Information.