Use of Email by Physicians

This section will:
• Summarize the benefits and risks associated with the use of email in the clinical context. • Identify key considerations required when using email for transmitting personal information. • Identify key considerations required if planning to use email communication with patients.

The use of email for communication in medical offices has in some cases become as common as fax. Email is a quick and efficient method for sharing information between providers and between providers and patients. When used in addition to face-to-face communication, email can enhance the patient-provider relationship. It can reduce non-essential office visits and save time otherwise spent communicating by phone. Email permits both parties to read and respond when it's convenient, and it also allows supporting documents to be attached, if necessary.

Steps must be taken to reduce the risks associated with email communication and ensure that reasonable safeguards are in place to protect personal information exchanged via email.

What are the risks?

In general, any type of email communication has some embedded risks:

1. An email message, because it is usually not encrypted, can be intercepted. It can also be altered and forwarded to unintended recipients or delivered to the wrong address.
2. Email messages containing personal information can be sent or received from unsecure locations such as a publicly accessible computer or a home computer. These messages could be retained on the home computer or in files maintained by Internet service providers. People other than the intended recipient may have access to the email account.
3. Attachments associated with an email may contain viruses that could cause serious damage to computer systems.
4. Email backup services and organizational retention rules may expose the information beyond what was intended.
5. The information being emailed may leave Canada during the email transition and become subject to other legislation or be affected the absence of legislation.

There are several additional risks to patient-provider email communication:

1. It can be difficult to confirm the identity of the patient in an email request. A patient's name without additional identifiers may be insufficient as patients may have similar names and email addresses.
2. If a patient does not receive a response in a timely manner, there may be adverse health consequences such as not getting the medical help needed on time.
3. A certain level of patient literacy is required for the email exchange to be beneficial and efficient.
4. The content of an email can be misinterpreted, which could lead to adverse health consequences or even a complaint or legal action if the patient's perception is one of inadequate or ineffective communication.

How to Reduce the Risks

Email sent to another physician or hospital about urgent or significant patient issues should not be considered a substitute for effective and efficient communication as there is no assurance the recipient will access the account regularly.

Before emailing personal information, take the following precautionary steps:

1. Confirm that you have the correct email address for the intended recipient. Verify email addresses regularly as they are not always intuitive, can be duplicated, and frequently change.
2. Where feasible, the recipient of the email should be contacted and informed that confidential information is being sent. Have the recipient call back to confirm receipt.
3. When emailing sensitive personal information consider using unique identifiers or codes to protect the identity of the individuals involved. Unsecured email messages can be read during transmission.
4. Ensure that confidential and sensitive personal information sent by email is encrypted with access provided only to authorized individuals who have the access code.
5. Add a confidentiality disclaimer to email messages that states that the content is confidential and only intended for the stated recipient. It should also state that anyone receiving the email in error must notify the sender, and return or destroy the email as per the request of the sender.
6. Protect any attached documents with a strong password and notify the recipient by phone of the password.
7. As sender, be aware of the security of the receiving email account and who has access to it.
8. Ensure that each email inbox used to send or receive messages has a secure password known only by the individual authorized to access that inbox.
9. Never use email distribution lists to send personal information.

Finally, While PIPA does not include the FIPPA provisions regarding prohibition of storage and access to personal information from outside Canada, it is recommended that physicians avoid the disclosure of personal identifiable information outside of Canada and prohibit access to such records from outside Canada without expressed patient consent.

Before agreeing to implement patient-physician email communication, take the following steps:

1. Thoroughly consider the advantages and disadvantages of email communication with patients before offering this service.
2. Where possible, use alternative and secure methods of delivering personal information, particularly sensitive information. Do not email sensitive information such as personal health information unless absolutely and immediately necessary.
3. Establish an office policy on email and ensure that:
    a. It includes criteria for the patient-provider communication, acceptable use, email etiquette, and management of email documentation as part of the patient's medical record.
    b. Staff are trained on the appropriate use of email and maintenance of emailed documents.
4. Develop policies and procedures:
    a. To inquire about the patient's literacy and ability to use email effectively.
    b. To obtain the patient's consent to the use of email as a method of communication.
    c. To educate patients about the appropriate use of email for this purpose.
    d. On termination of a patient from email communication.
5. Address security risks by implementing encryption technologies, email access codes, and other measures to protect against unauthorized access.

If an email containing personal information is sent to the wrong address or recipient, follow these steps:

1. Contact the person responsible for privacy compliance in the office.
2. Follow procedures for managing privacy breaches. (See the section Responding to a Privacy Breach—Key Steps for Physicians.)

If someone asks the physician office to email his or her personal information, be sure to follow these steps:

1. Identify the person making the request with certainty and advise him or her of your preference to provide the data in a more secure fashion (e.g., photocopies sent by mail or courier).
2. Explain how emailing personal information can result in accidental disclosure or interception by other people not intended to receive the information.
3. Explain the precautions that have been taken to reduce the risks and ensure the person consents before emailing the personal information.

Maintenance of Email Documents

When planning an email maintenance policy, consider the following:

1. Do not make or retain more copies of email communications than needed.
2. Securely destroy extra copies that are no longer needed.
3. Ensure that personal health information emailed becomes part of the patient's medical record and follow appropriate retention guidelines.