Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Fact Sheet

Communicating Personal Health Information by Email

September 2016

Email is one of the dominant forms of communication today. Individuals and organizations have come to rely on its convenience, speed and economy for both personal and professional purposes. Health information custodians (custodians) are no exception. While email offers many benefits, it also poses risks to the privacy of individuals and to the security of personal health information. It is important for custodians to understand these risks and take steps to mitigate them before using email in their professional communications.

OBLIGATIONS UNDER THE PERSONAL HEALTH INFORMATION PROTECTION ACT

The *Personal Health Information Protection Act* establishes rules for protecting the privacy of individuals and the confidentiality of their personal health information, while at the same time facilitating effective and timely health care. Custodians have a duty to ensure that health records in their custody or control are retained, transferred and disposed of in a secure manner. They are also required to take reasonable steps to protect personal health information against theft, loss and unauthorized use or disclosure.

UNDERSTANDING THE RISKS

Like most forms of communication, email entails an element of risk. An email can be inadvertently sent to the wrong recipient, for example, by mistyping an email address or using the autocomplete feature. Email is often accessed on portable devices, such as smart phones, tablets and laptops, which are vulnerable to theft and loss. An email can also be forwarded or changed without the knowledge or permission of the original sender. Email may also be vulnerable to interception and hacking by unauthorized third parties.

Personal health information is sensitive in nature. Its unauthorized collection, use or disclosure may have far-reaching consequences for individuals, including stigmatization, discrimination and psychological harm. For custodians and their agents, privacy breaches may result in disciplinary proceedings, prosecutions and lawsuits. In addition, such privacy breaches may result in a loss of trust and confidence in the entire health sector that was entrusted to protect this sensitive information.

ADDRESSING THE RISKS

Technical, Physical and Administrative Safeguards

Custodians must implement technical, physical and administrative safeguards to protect personal health information. This requirement applies to any email communications involving this type of information.

Technical safeguards include:

- encryption for portable devices
- strong passwords, and
- firewalls and anti-malware scanners

Physical safeguards include:

- restricting office access, using alarm systems, and locking rooms where equipment used to send or receive health information by email is kept, and
- keeping portable devices in a secure location, such as a locked drawer or cabinet, when they are unattended

Administrative safeguards include:

- providing a notice in an email that the information received is confidential
- providing instructions to follow if an email is received in error
- communicating by email from professional, rather than personal accounts (personal accounts may have weaker security levels and may be more susceptible to compromise)
- confirming an email address is up to date
- ensuring that the recipient's email address corresponds to the address proposed to be sent
- regularly checking preprogrammed email addresses to ensure that they are still correct
- restricting access to the email system and to email content on a need-to-know basis
- informing individuals of any email address changes
- acknowledging receipt of emails, and
- recommending that individuals implement the above safeguards, including that individuals communicate by email at an email address that is password protected, and is accessible only by them

Custodians should also ensure compliance with the safeguards specified in any other policies and procedures, such as those related to bringing your own device to the workplace.

For further information on safeguarding personal health information, please see our fact sheet, ***Safeguarding Personal Health Information***.

Email Encryption

An important and effective way to mitigate the risks associated with emailing personal health information is through the use of encryption technology. Encryption scrambles the contents of an email so that only those with access to a secret key or password can unscramble and read it. Encryption minimizes the risk of unauthorized collection, use or disclosure of information. The use of encryption in the context of email communication among custodians and email communication between custodians and their patients is discussed below.

For further information on encryption, please see our fact sheets, ***Encrypting Personal Health Information on Mobile Devices*** and ***Health-Care Requirement for Strong Encryption***.

Email Communication Among Custodians

The IPC expects that email communication of personal health information among custodians will be secured from unauthorized access by use of encryption, barring exceptional circumstances. Most secure email solutions involve end-to-end encryption, allowing the sender to be confident that only the intended recipient will read the email. The recipient can also be confident that the message is genuine and originated from the sender. For example, the ONE Mail service offered by eHealth Ontario allows registered health care professionals to send and receive personal health information in an encrypted manner.

However, there may be exceptional circumstances where the communication of personal health information between custodians through encrypted email is not practical. For example, in emergency or other urgent circumstances, custodians may determine that the use of unencrypted email is the most timely and practical means of communicating information. Custodians should also look to their health regulatory colleges for any applicable guidelines, standards or regulations on the use of unencrypted email to communicate personal health information.

Email Communication Between Custodians and Their Patients

Where feasible, custodians should use encryption for email communication with patients. Encryption technology is becoming more widely available and easier to use. Increasingly, patient portals and electronic medical record systems include encrypted messaging applications as a feature.

If encryption is not feasible, custodians should determine whether it is reasonable to communicate with their patients through unencrypted email. Custodians should consider the following:

Characteristics of the information

What type of information will the custodian be sending to the patient? While all personal health information is sensitive, the degree of sensitivity may vary. For example, the time and date of an appointment may not be as sensitive as diagnostic information contained in an individual's health record.

Volume of information and frequency of emails

As the volume and frequency of emails increase, so does the risk. Will the email include a large volume of personal health information? Is the custodian sending the information only one time, or on a frequent, continuing basis?

Purpose of transmission

Is the custodian considering using email for administrative purposes, such as sending appointment reminders, for education and health promotion, such as providing general health resources or for individual care, such as answering follow-up questions?

Patient expectations

What are the patient's expectations as to how the custodian will communicate with him or her?

Availability of alternative methods and their associated risks

What are the available alternative methods of communication? The custodian should assess the risks to privacy and confidentiality posed by each method and select the one that carries a risk level that is proportional to the harm that could result from a privacy breach.

Emergency and other urgent circumstances

Is the custodian faced with an emergency or other urgent circumstance? Is unencrypted email the timeliest and most practical means for the custodian to communicate information necessary for the provision of health care to the individual or to prevent harm?

Having considered all of the above, the custodian must be satisfied that the use of unencrypted email is reasonable. If a custodian is not satisfied that it is reasonable, then the custodian should not communicate with patients by this method.

Email Policy

Custodians should develop and implement a written policy for sending and receiving personal health information by email. The policy should address when, how and the purposes for which this information may be sent and received by email, as well as any conditions or restrictions on doing so. The policy should also set out what types of information may be sent and received by unencrypted email and the circumstances in which the custodian will use unencrypted email.

Notice and Consent

Custodians must notify their patients about their written email policy and obtain their consent prior to the use of unencrypted email. The consent should be in plain language and indicate the types of information that may or may not be communicated by unencrypted email, the risks of using unencrypted email and the circumstances where the custodian will use unencrypted email. For example, custodians may limit the use of unencrypted email to the scheduling of appointments only and have a policy of not sending or receiving any clinical information via unencrypted email. Custodians may wish to provide different consent options, allowing individuals to choose the circumstances where they agree to the use of unencrypted email.

Both notice of and consent to unencrypted email communications can occur in a variety of ways. For example, if patients provide their email addresses in writing, such as by completing a form, the form can include information on the risks involved in unencrypted email communications and allow them to consent to its use. This can also take the form of verbal discussion, if and when individuals provide their email addresses orally to the custodian.

Data Minimization

Even if a patient agrees to communicate by email, this does not mean that all personal health information should be sent by this method. The custodian still has a duty to limit the amount and type of personal health information included in an email. Custodians should also consider how they will respond to requests from individuals to put restrictions on the use of email.

Retention and Disposal of Personal Health Information

Custodians are required to retain and dispose of personal health information in their custody or control in a secure manner. This requirement applies to information contained in email communications.

Custodians should store personal health information on email servers only for as long as is necessary to serve the intended purpose. For example, if an email communication has already been documented in the patient's record, it may not be necessary to retain duplicate copies of the information on email servers. Likewise, custodians should ensure that all copies of emails containing personal health information on portable devices are deleted when they are no longer needed and have already been documented in the individual's record.

Encrypting portable devices prevents unauthorized access to stored information in case of theft or loss. Personal health information can also be safeguarded by encrypting backups, including those located offsite.

For further information, please see our fact sheet, ***Safeguarding Personal Health Information*** and ***Secure Destruction of Personal Information***.

Training and Education

Comprehensive privacy and security training is an essential tool to reduce the risk of unauthorized collection, use and disclosure of personal health information. Custodians should ensure their employees and other agents are provided with, and are required to undergo, initial and ongoing privacy and security training, including training on the policy and procedure for sending and receiving personal health information by email.

Privacy Breach Management

Custodians should have a privacy breach management protocol in place. The protocol should address identification, reporting, containment, notification, investigation and remediation of actual or suspected privacy breaches.

The IPC does not consider the loss or theft of an electronic device containing encrypted personal health information to be a privacy breach. However, whether or not the information is encrypted, custodians should require their agents to report any such loss or theft. This will enable custodians to determine, on a case-by-case basis, whether the information was properly protected.

For further information on privacy breaches, please see, ***What to do when Faced With a Privacy Breach: Guidelines for the Health Sector***.