Advisory for

Communicating with Patients Electronically

Custodians have a duty to protect the privacy of patients and the confidentiality of health information in their custody or control, as outlined in section 60 of the *Health Information Act* (HIA). The risks of communicating with patients electronically must be considered.

Responsibility for safeguarding health information cannot be transferred to a patient by having a patient sign a consent form or disclaimer to accept the risks associated with electronic communications.

Electronic communications with patients can improve efficiency by:

- Sending appointment reminders
- Setting up specialist appointments
- Notifying patients about a new service offering
- Following up with patients on a treatment plan

Risks of Electronic Communications

Electronic communications are susceptible to certain risks, such as:

- Interception: If accounts or devices are shared or accessible by multiple people, the wrong recipient may read the message.
- Misdirection: Patients may have similar names or account addresses and a message may be sent to the wrong patient.
- Alteration: Test results can be sent to a patient who may alter the document and send the changed results to another health care provider, which will appear to be trusted health information.
- Loss: If a service provider manages cloud storage of emails or other electronic records, when there is an outage, a security breach, or a service provider goes out of business or is taken over by another entity, access to health information may be lost. Additionally, certain security incidents may result in the loss of health information entirely.
- Inference: The name and nature of a health service provider on its own may reveal health information of an individual if other individuals, such as friends or family members, have access to or can see notifications on a patient's device.

Mitigating Risks

HIA requires that custodians take reasonable steps to maintain safeguards to protect the confidentiality of health information and to protect against any threats to the security of health information, to the loss of health information, and to any potential breaches of health information (e.g. unauthorized use, disclosure, modification or access to health information).

In light of the various risks associated with communicating with patients electronically, consideration must be given to protecting health information, including:

- Managing electronic records: There are additional challenges for the secure storage and maintenance of electronic communications.

Office of the Information and Privacy Commissioner of Alberta

Updated June 2019
Published August 2012

- Identification: Electronic communications raise questions about how a patient can verify and trust that the sender is a clinic or custodian.
- Device management: Electronic communication is often done with the use of mobile devices. Safeguards around how a device is stored, whether devices are used outside a clinic or office environment, who owns the device, whether health information is stored in a cloud or on a device itself, and appropriate uses of devices outside of a clinic or office environment must be considered.
- Encryption: Diagnostic, treatment and care information should be encrypted. A message itself, attachments or a combination of these may require encryption. If mobile devices are used to store health information, those devices must be encrypted.

  Consider programs or technical advice to help in setting up processes and procedures for encrypting electronic communications and devices.
- Limiting amount of health information: When sending or receiving health information that does not include clinical details, limit the amount of health information sent electronically; limit the amount of health information collected using web forms or electronic templates; and tell patients exactly what will and what will not be communicated electronically, in addition to how messages containing clinical information will or will not be accepted.
- Policies: There are certain policies and procedures that should be considered, such as policies that address:
  - Communicating with patients electronically and acceptable uses of mobile devices
  - Training staff on secure electronic communication (e.g. training on encryption methods)
  - Determining how to manage records sent by patients (e.g. if a patient sends unsolicited health information via email, how will it be managed?)
  - Regularly confirming patients' preferred methods of communication and contact information (e.g. ensure email addresses are up to date and that a patient prefers to receive certain updates via email)
  - Notifying patients of risks when communicating electronically (e.g. whether another individual has access to certain accounts or electronic devices)

Policy and PIA Requirements

HIA requires that a custodian establish or adopt policies and procedures to facilitate implementation of the Act (section 63). It also requires a custodian to submit a privacy impact assessment (PIA) to the Office of the Information and Privacy Commissioner before implementing a new practice or information system – or when making changes to an existing practice or system – that collects, uses or discloses individually identifying health information (section 64).

If a custodian is considering electronic communication tools to correspond with patients they must have appropriate risk mitigation strategies and policies. A PIA helps to manage privacy risks when communicating with patients electronically before such tools are implemented.