Office of the
Information and Privacy
Commissioner of Alberta

#410, 9925-109 Street Edmonton, Alberta Canada T5K 2J8 ph(780) 422-6860 fax(780) 422-5682

August 2012

HIA Practice Note #5

Communicating with patients via email: Know the risks

As a custodian under Alberta's *Health Information Act* (HIA), you have a duty to protect the privacy of your patients and the confidentiality of health information in your custody or control. You must consider the risks of communicating with patients electronically.

Emailing patients can improve health outcomes and overall efficiency. Examples include:

- sending appointment reminders
- setting up specialist appointments
- offering a new service, such as a smoking cessation program, or diabetes clinic
- following-up with patients on a treatment plan

Email offers many benefits, but remember, as a custodian you must consider patient privacy.

The Risks

Email is susceptible to the following risks:

Interception -- you send an email to an address used by a patient and her family. A family member receives and reads the email.

Misdirection -- two of your patients have similar email addresses. You send an email containing sensitive health information to the wrong patient.

Alteration -- you send test results to a patient with a chronic condition via email. The patient alters the results and provides them to another care provider as trusted health information

Loss -- you save emails offsite with your 'cloud' email service provider. The email provider goes out of business and you lose access to valuable health information or refuses to provide you with your data when you want to change your service provider.

Inference -- you send an appointment reminder to your patient. The name and nature of your practice reveal health information about your patient to family members with access to the patient's email account.

Mitigating Risks

As a custodian, implementing reasonable privacy safeguards when emailing patients is your responsibility. Safeguards should align with the sensitivity of the health information. Encrypt or limit the health information sent via email.

Encrypt

If you need to send or receive detailed diagnostic, treatment and care information, encryption is the best technical safeguard. Encryption uses mathematical algorithms to scramble information so it can only be read with an encryption key. Depending on the risks you identify, you may decide to encrypt the communication channel, the message itself, attachments, or some combination of these.

Encryption and digital signatures (which employ encryption technology) ensure your message is received by the intended recipient, is not altered and is not intercepted and read by unauthorized parties.

Encrypted email can be complicated to set up, seek technical advice or consider an outsourced encrypted email solution (managed through a contract that meets HIA requirements).

...or Limit

The following safeguards may be sufficient when sending/receiving *limited* health information that does not include clinical details (consider your own unique circumstances and make your own assessment):

- Limit the amount of health information in emails
- Limit the amount of health information you collect using web forms or electronic templates
- Advise your patients exactly how you will communicate with them via email and let them know you will not accept emails containing detailed clinical information

Policies and Training

Whether you encrypt or limit health information exchanged electronically, consider the following administrative controls:

- Establish a policy on communicating with patients via email
- Train staff on secure email use (if you tell your staff to encrypt emails, train them how to do it properly).
- Determine how you will manage records generated in patient emails. For example, how will you manage unsolicited health information sent to you by patients?
- Regularly confirm your patients' email addresses. When confirming, have your patients consider email risk, whether they want to receive emails and who else

may have access to their email account. Keep a record of the confirmation you receive from the patient.

Privacy Impact Assessment

The HIA requires that custodians submit a Privacy Impact Assessment (PIA) to the Information and Privacy Commissioner before implementing a new administrative practice or information system that collects, uses or discloses identifying health information. Completing a PIA will help you manage privacy risks when communicating with patients via email.

Quick tips

1. Stop and think - is email the best way to communicate with your patient given the sensitivity of the health information you are sending?

2. Is another channel available? For example, can you use the encrypted messaging in another system or use a secure patient portal in your electronic medical record?

3. Limit the amount of health information you send and receive via email to only what is essential.

4. If you must send identifying diagnostic, treatment and care information, encrypt your email.

5. Double-check email addresses, cc and bcc fields and attachments before sending.

6. Before you start emailing patients, do a privacy impact assessment and submit it to the Information and Privacy Commissioner. Read more about PIAs here.

Email Communication FAQ's