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

Email Communication FAQs

Instead of limiting the amount of information or encrypting, can I mitigate risk by having patients sign a consent form or disclaimer where patients accept the risks associated with email use?

Custodians are responsible for ensuring reasonable safeguards are in place to protect against reasonably anticipated risks to privacy. This responsibility cannot be transferred to the patient. It is a good practice to regularly re-confirm that patients want to be contacted via email, to verify their email address and to inform them of possible risk, but this does not transfer responsibility for securing your emails to the patient.

Can email be integrated into an existing EMR?

Yes, custodians can add email to their existing EMRs after completing the privacy impact assessment (PIA) required by section 64 of the HIA.
Changes to the Qualified Service Provider (QSP) EMR solutions under the Physician Office System Program (POSP) are addressed through a formal change management process, which includes completion of the required PIA on behalf of all physicians using that solution. QSP vendors can only add email to their EMR after all required PIAs have been accepted.
Custodians who make changes to an EMR solution outside the POSP program must update their existing PIA to reflect the new risks to privacy introduced by email and how these risks will be mitigated.

Is our privacy risk different if we text our patients instead of using email?

Text messaging shares many of the same risks as email including interception, misdirection, alteration, loss and inference. It does however pose some additional risks that custodians should assess before offering this service to patients, including:
Records management – how will you maintain a record of the information communicated to your patients via text?
Identification – How will the clinic identify itself to their patients via text? If you receive texts from patients how will you readily identify them?

It is important for custodians to consider all of the risks associated with implementing text messaging as a tool to communicate with patients and to put in place appropriate risk mitigation strategies for these risks prior to implementation. Submit a Privacy Impact Assessment to the OIPC for review and comment before you implement.

Do mobile devices such as smart phones and tablets pose different risks with respect to emailing patients?

Mobile devices pose some additional risks to the privacy and security of health information, depending on how they are used to transmit email. Custodians should ask themselves the following questions:
Physical Safeguards - How will the device be stored? Is there an increased chance of theft or loss? Will the device be used outside of the clinic?
Technical Safeguards - Will health information be stored on the device? If so, the health information needs to be encrypted.
Administrative Safeguards – Do my current policies and procedures address appropriate use of this device? How do I inform staff about appropriate use of this device?

Investigation report H2006-IR-002 recommended that custodians encrypt mobile devices if they store identifiable health data.