Use of Email for Communicating Personal Health Information

The effective delivery of health care undoubtedly requires custodians to communicate using timely and efficient methods. While email may be a useful means of communication, it also involves an element of risk. An email can be inadvertently sent to the wrong recipient; it can be forwarded or changed without the knowledge or permission of the original sender; and it may also be vulnerable to interception and hacking by unauthorized third parties. Additionally, the personal health information being emailed may leave Canada during transmission, and may be subject to laws in other jurisdictions that have inadequate protections or no protections at all.

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, privacy breaches may result in disciplinary proceedings, prosecutions or lawsuits. In addition, such privacy breaches may result in a loss of trust and confidence in the entire health sector.

Section 15 of the *Personal Health Information Act* ("*PHIA*") requires that a custodian take reasonable steps to ensure that the personal health information in its custody or control is protected against theft; loss; unauthorized access, use or disclosure; and unauthorized copying or modification. It also mandates that records containing personal health information be retained, transferred and disposed of in a secure manner.

The communication of personal health information may only be carried out in accordance with the collection, use and disclosure provisions of *PHIA*. Inherent risks, associated with email should be addressed before using it as a method of communicating personal health information to clients or their substitute decision-makers. Custodians are responsible for ensuring reasonable safeguards are in place to protect against risks to privacy. This responsibility cannot be transferred to the patient. If email is to be used to communicate with patients/clients, in addition to the tips outlined below, it is a good practice to regularly confirm that patients want to be contacted via email, to verify their email address and to inform them of possible risks. Obtaining consent from the patient/client may mitigate but will not negate the consequences to a custodian of a privacy breach.

Prior to Sending Personal Health Information in an Email

PHIA establishes a right of access to and correction of personal health information. This includes personal health information which exists in email format. Custodians need to be aware that their email records are subject to any professional practice standards established by their profession, and, along with any other records of personal health information, email records could be subject to an investigation by the Commissioner if there is a complaint from an individual relating to any aspect of *PHIA*.

1. *Privacy Impact Assessments*
   - Prior to using email to communicate personal health information, consider doing a privacy impact assessment on the practice. For further guidance on privacy impact assessments, please see our guidance documents: Privacy Impact Assessments and PPIA/PIA Review Criteria or contact the OIPC.

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

2. *Develop written policies and procedures*
   - Policies surrounding sending personal health information via email should be developed in accordance with section 13 of *PHIA*.
   - Policies should include who is permitted to send emails containing personal health information, when personal health information may be sent via email, to whom personal health information may be sent, and the conditions under which an email containing personal health information may be sent. Policies should address the use of encryption, managed file transfer or other methods of ensuring email content is only accessible by the intended recipient.
   - Policies should also discuss procedures for receiving personal health information via email.
   - Employees and other agents should be provided with, and be required to undergo, initial and ongoing privacy and security training, including training on the policies and procedures for sending and receiving personal health information by email.

3. *Necessity*
   - Consider whether email is the best way to communicate the information and whether another, more secure method is available.

<u>Sending an Email Containing Personal Health Information</u>

1. *Limits*
   - Limit the amount of personal health information being sent to only what is necessary.
   - Ensure that no personal health information is in the subject line of the email.
   - Only place essential information in the body of the email.
   - Personal health information should be sent as an encrypted attachment.
   - Whenever possible, reduce the amount of sensitive information in the body of the email. For example, rather than disclosing a patient's prognosis or diagnosis in an email, instead refer generally to the contents – "a test" or a "procedure" and ask the recipient to refer to the encrypted attachment for further information.

2. *Security*
   - Ensure that personal health information is sent as a secure, locked (e.g. .pdf) attachment which requires a password to open.
   - Communicate the password to the recipient using a separate method.
   - Use a professional, as opposed to personal, web-based, email account to send the email. Personal accounts usually have weaker security and may be more susceptible to compromise.

3. *Verification*
   - Verify the email address with the intended recipient(s) and re-check the email addresses, cc and bcc fields and attachments before sending.
   - Autocomplete or autofill options should be turned off to avoid errors.
   - Read/received/delivery receipts should be used where possible.
   - Add a disclaimer to your signature that indicates that the email is confidential and intended only for the intended recipient. It should also instruct anyone who receives the email in error to delete or shred the misdirected mail and notify the sender.

4. *Maintain copies*
    - Copies of the email and attachments should be maintained in the client file. The date, time, addressee of the email should be apparent.

Privacy Breaches Involving Email

It is essential that custodians follow the privacy breach protocol if a breach occurs. Custodians are also required to inform the Commissioner of a material breach, as defined in section 15(4) and regulation 5 of *PHIA*.

The privacy breach protocol has 4 key steps: containment, evaluation, notification and prevention.

1. *Containment*
    - Recover the misdirected email or ensure that any hard copies are securely disposed of. Direct that any electronic copies be permanently deleted from both the recipient's inbox and trash.
    - Instruct the recipient not to download or distribute the email and attachments.
    - Request that the recipient confirm in writing that these instructions have been followed.
    - Ensure that no further emails are sent to that email address unintentionally while the investigation is on-going.
2. *Evaluation*
    - Determine precisely what personal health information was contained in the email, the patients to which the information relates and whether any of the information was encrypted to prevent access.
    - Identify the cause of the breach.
3. *Notification*
    - Notification should occur as soon as possible following a breach, unless the custodian reasonably believes that the breach will not have an adverse impact upon the individual affected. In determining whether a breach will have an adverse impact, custodians should consult section 15(7) of *PHIA.*
    - Direct notification is preferable.
    - Notification should include: date of the breach; a description of the breach and the information involved; any identified risks; the steps taken in relation to the investigation and breach containment; any identified future steps; any steps the individual can take; as well as any steps the custodian is offering to assist the individual in mitigating the harm.
    - The notification should also contain the contact information for the custodian and for the OIPC, along with informing the person of the right to file a privacy complaint.
4. *Prevention*
    - In relation to errant emails prevention methods may include: disabling autocomplete/autofill options; deleting autocomplete/autofill and suggested contacts lists; developing and implementing policies regarding the use of email to send personal health information; ensuring that all personal health information being sent via email is encrypted; and training staff in the use of the email system and their obligations under *PHIA*.