Safeguard

A QUARTERLY NEWSLETTER PUBLISHED BY THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

VOLUME 1, ISSUE2 AUGUST 2017

CONTACT INFORMATION

Office of the Information and Privacy Commissioner
3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8
Tel: (709) 729-6309
Fax: (709) 729-6500
Toll Free in Newfoundland and Labrador: 1-877-729-6309
E-mail: commissioner@oipc.nl.ca
www.oipc.nl.ca

"Thus, at least in part, medical records contain information about the patient revealed by the patient, and information that is acquired and recorded on behalf of the patient. Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that goes to the personal integrity and autonomy of the patient."

- Justice La Forest *McInerney v. MacDonald*, [1992] 2 SCR 138 (SCC)

APSIM Conference 2018

We are pleased to announce that we will once again be offering a FREE Access, Privacy, Security and Information Management conference in early May 2018.

Last year's APSIM conference was very well received and we intend to provide the same quality of content you have come to expect with experienced and knowledgeable presenters and a diverse range of topics.

This conference will be of interest to all professionals who work in the information management, security and access and privacy fields. The topics covered will capture the interest of all the communities impacted by the *Access to Information and Protection of Privacy Act, 2015* and the *Personal Health Information Act*.

We hope to see you there!

OIPC REMINDERS AND UPDATES

New Senior Access & Privacy Analyst

Please join us in congratulating Janet O'Reilly on becoming our new Senior Access & Privacy Analyst. Many of you already know Janet through her work on investigative files and as an educational ambassador for this Office. She is excited to continue to work with you in this new role.

Important Email Addresses

Custodians are reminded to use the following email address to report privacy breaches:

breachreport@oipc.nl.ca

Guidance Documents

We will be developing and publishing *PHIA* guidance documents to assist custodians in better understanding their roles and obligations and interpreting *PHIA*. Keep an eye on Safeguard and our website for publication updates.

FAXING AND EMAILING PERSONAL HEALTH INFORMATION

The use of fax or email to send or receive personal health information is commonplace but extra care and precaution must be taken so as to avoid misdirected records. As the sensitivity of the contents increases, the appropriateness of using unencrypted fax or email decreases. Below are some quick tips for avoiding inadvertent privacy breaches.

Fax

- Confirm the recipient's fax number before you hit the send key.
- Regularly review pre-programmed fax numbers and update regularly.
- Use a fax cover sheet which contains a disclaimer informing the recipient to notify the sender and destroy the records if they are not the intended recipient. Do not include personal information on the cover page.
- Locate your fax machine in a secure area.
- Set a designated time to send the fax and request that the recipient immediately retrieve the fax.
- Call to verify receipt of the fax. Ensure all pages have been received.
- If sending via fax to email, use a password and encrypt the transmission.
- If available, use features that require recipients to enter a password to obtain the sent fax.
- Remove documents, both sent and received, from the fax machine immediately.
- Maintain a record of fax transmission by keeping transmittal records for a set period of time.
- Limit the amount of personal information you include or, if possible, de-identify the records.
- Create policies regarding the type of information that can be sent via fax and when fax is a permissible method of transmission. Ensure staff is aware of and trained on these policies.

Email

- Confirm the full email address before you hit send.
- Delete pre-populated addresses.
- Add a disclaimer signature line informing the recipient to notify the sender and destroy the records if they are not the intended recipient.
- Send a test email first to ensure you have the right person.
- Use encryption to protect the content of the email and its attachments.
- Call ahead to advise recipient the email is being sent.
- Call to verify receipt of the email.
- Use the delivery receipt feature.
- Do not include personal information in the subject line.
- Be aware of who has access to the account to which you are sending the email.
- Never use a personal email account to send emails containing personal health information., unless there is no other alternative.
- Limit the amount of personal information you include or, if possible, de-identify the records. create policies regarding the type of information that can be sent via email and when email is a permissible method of transmission. Ensure staff is aware of and trained on these policies.

THE CIRCLE OF CARE

A custodian of personal health information may rely on continuing implied consent for the collection, use and disclosure of personal health information within the "circle of care".

The term "circle of care" is defined in *PHIA,* at section 24(3):

> *...[T]he expression "circle of care" means the persons participating in and activities related to the provision of health care to the individual who is the subject of the personal health information and includes necessarily incidental activities such as laboratory work and professional consultation.*

The circle of care is a phrase used to describe those individuals who are providing health care to a patient and may assume to have that patient's implied consent to collect, use or disclose personal health information for the purpose of providing health care to that individual.

A custodian may only deal with an individual's personal health information within the circle of care (i.e. may only assume to have an individual's continuing implied consent to collect, use or disclose personal health information) where **all** of the following conditions are satisfied:

1. The custodian must fall within <u>one of the categories of custodians</u> authorized to rely upon implied consent:

   i) a health care professional, when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;
   ii) a health care provider; or
   iii) a person who operates:
      a. a health care facility,
      b. a licensed pharmacy as defined in the *Pharmacy Act, 2012*,
      c. an ambulance service, or
      d. a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider.

2. The information to be collected, used or disclosed by the custodian must be personal health information in accordance with *PHIA* and must have been <u>received from the individual, his or her substitute decision-maker or another health information custodian</u>.

3. The health information custodian must have received the personal health information that is being collected, used or disclosed for the purpose of providing or assisting in the <u>provision of health care to the individual to whom it relates</u>.

4. The purpose of the collection, use or disclosure of personal health information by the health information custodian must <u>only be for the provision of health care or assisting in the provision of health care to the individual</u>.

THE CIRCLE OF CARE (CONTINUED)

5. Regarding disclosure of personal health information within the circle of care, the disclosure by a custodian must be made for the sole purpose of providing health care to the individual.

6. The implied consent of the individual must be valid and the individual must not have expressly withheld or withdrawn their consent to the collection, use or disclosure.

   In order for implied consent to be considered valid, it must be reasonable to believe that the individual is aware of the purpose of the collection, use or disclosure and knows that they can either give or withhold consent. It is, in turn, reasonable to believe that an individual knows the purpose of the collection, use or disclosure if the health information custodian posts or makes readily available an adequate notice generally describing these purposes in a location where it is likely to come to the individual's attention or provides the individual with such a notice in accordance with section 20(2).

   Section 28 of *PHIA* permits an individual to expressly withdraw their consent to the collection, use or disclosure of his or her personal health information (unless the collection, use or disclosure is permitted or required by *PHIA* to be made without their consent) by providing notice to the custodian. An individual may withdraw their consent for collections, uses or disclosures that occur within the circle of care; however, custodians may continue to act on the basis of implied consent unless and until an individual expressly withdraws their consent.

   In most circumstances, if an individual decides to withhold or withdraw consent, *PHIA* requires the requesting custodian to be notified by the disclosing custodian that it is prevented from disclosing all of the information that is considered to be reasonably necessary for the provision of health care (i.e. that the requesting custodian is receiving no information, where information does exist, or only partial information where additional information exists).

General Limiting Principle

In addition to the above six conditions, *PHIA* requires that a custodian not collect, use or disclose personal health information if other information will serve the purpose. Custodians are also required to not collect, use or disclose more personal health information than is reasonably necessary for the intended, authorized purpose. These general limiting principles apply even where a health information custodian is entitled to rely on an individual's implied consent.

OIPC *PHIA* REPORTS

Since the proclamation of *PHIA* on June 4, 2008, this Office has issued two *PHIA* Access Reports and four *PHIA* Privacy Reports.

ACCESS

Report AH-2012-001 – Eastern Health

The Complainant sought access to a copy of a diagnostic test he had undergone at a local hospital, consisting of a single page. Eastern Health, in accordance with its fee schedule, informed the Complainant that a copy of the record would cost $50.00 plus tax. Under section 57 of *PHIA*, a custodian is permitted to charge a "reasonable fee". The Commissioner found that the $50.00 fee to provide individuals with their own personal health information was unreasonable and recommended that individuals be charged a maximum fee of $25.00 for requests of up to 50 pages. After the first 50 pages, the Commissioner recommended a photocopying fee of no more than $0.25 per page. The Commissioner also strongly recommended that personal health information be provided to individuals free of charge at the point of care, except where the requested information is not easily located or voluminous in nature and that the fee be waived or substantially reduced in all cases where it truly represents a barrier to access.

Report AH-2014-001 – Eastern Health

The Complainant requested correction of certain personal health information in a clinical report. Specifically, the Complainant claimed that he had not made statements attributed to him in the report. Eastern Health refused to grant the request for correction. As this was the first occasion upon which the Commissioner addressed the provisions of *PHIA* dealing with the correction of personal health information, the Commissioner adopted the analysis used by the Alberta Commissioner. The Commissioner found that the disputed portions of the clinical report consisted "professional observation" within the meaning of section 62 of *PHIA* and concluded that the custodian was not required to correct such information. However, the custodian was required to annotate the record with the correction that had been requested, but not made.

PRIVACY

Report PH-2012-001 – Custodian Not Named

A Complainant filed a Privacy Complaint with this Office against a massage therapist as a Custodian under *PHIA*. The Complaint alleged that the Custodian lost a file containing the Complainant's personal health information. The Commissioner found that the Custodian breached sections 13, 15, 19 and 20 of *PHIA*, as she had no policies and procedures in place regarding her collection, use and disclosure of personal health information, nor any of the required notice materials. The Commissioner recommended that the Custodian take immediate steps to safeguard the personal health information in her possession, develop and implement proper policies and procedures and post or provide notice materials as required by *PHIA*. The Commissioner also recommended that the Custodian complete the *PHIA* Online Education Course offered by the Department of Health and Community Services.

OIPC *PHIA* REPORTS (CONTINUED)

Report PH-2013-001 – Western Regional Health Authority

Two separate individuals filed Privacy Complaints under the *Access to Information and Protection of Privacy Act* alleging that their personal health information was not adequately protected, was improperly used, and was improperly disclosed. The complaints were broad in scope, expressing concern over the number of people who had access to patients' personal health information, what personal health information could be accessed, and for what reasons that access could occur. Specifically, the complaints were directed at concerns about the electronic records system in use by Western Health, known as Meditech. Subsequent to receipt of the complaints by the OIPC, *PHIA* was proclaimed into law and, to ensure that the recommendations were useful and relevant, the files were processed under *PHIA.* The Commissioner found that the electronic system being used by Western Health for employee access to personal health information did not meet the requirements and standards of *PHIA*. The Commissioner made a number of recommendations to better ensure Western Health's compliance with *PHIA.*

Report PH-2016-001 – Eastern Health

An intentional privacy breach occurred at Eastern Health when an unknown person inappropriately accessed and printed personal health information from the Meditech account of a doctor at Eastern Health. This information was then anonymously sent to the Department of Health and Community Services and the College of Physicians and Surgeons. It could not be proven who committed the breach, so no charges were laid under section 88 of *PHIA.* The Commissioner found that Eastern Health had taken reasonable administrative and technical security measures to protect personal health information as required by section 15 of *PHIA* and the breach appeared to have been perpetrated by someone who chose to ignore clear rules and policies. This person was able to inappropriately access the information through the account of another doctor when he inadvertently failed to log out of his computer session, contrary to Eastern Health policy. The Commissioner recommended that Eastern Health review best practices for automatic log out times and implement an appropriate standard consistent with privacy best practices and professional practice requirements. The Commissioner also recommended that Eastern Health remind employees of the importance of logging out of computer sessions and of the consequences for failing to do so.

Report PH-2017-001 – Morneau Shepell Ltd.

An individual complained that personal health information collected during a medical assessment for the purpose of a fitness certificate was improperly used and disclosed. The Complainant also alleged that there had been a failure to adequately protect his personal health information. The Commissioner determined that the occupational health services provider that collected the personal health information was a custodian under the provisions of *PHIA*. The Commissioner found that there had not been an improper use or disclosure of the Complainant's personal health information. Furthermore, there had not been a failure by the custodian to adequately protect the personal health information of the Complainant.

Key Steps in Responding to Privacy Breaches

STEP 1: *Contain the breach*. Do what is necessary to limit the breach and begin your investigation. Notify internal privacy and security personnel, the OIPC and the police if necessary.

STEP 2: *Evaluate the risks.* Identify the information involved and the sensitivity of the information. The more sensitive the information, the higher the risk. Identify the cause and extent of the breach including number of victims and the number of recipients, the identity of the recipients, the risk of further access, use or disclosure, whether the information was lost, stolen or accessed, whether the information was encrypted, whether the information was recovered, and whether the breach was an isolated incident. Identify the type of harm that may occur including, but not limited to, physical safety, identity theft, loss of business, emotional distress or damage, loss of trust, loss of contracts, and financial losses.

STEP 3: *Notification.* Notification should occur as soon as possible following a breach. Direct notification is preferable, however, multiple methods may also be used. Notification should include: date of the breach, a description of the breach and the information involved, any identified risks, the steps taken to date relating to the investigation and breach containment, as well as any identified future steps, any steps the individual can take to mitigate the harm, the contact information for the custodian and the contact information for the OIPC along with notification of the right to file a Privacy Complaint. Review section 15 of the *PHIA* for notification requirements.

STEP 4: *Prevention*. Evaluate the physical, technical, administrative and personnel safeguards currently in place and augment them accordingly to prevent future breaches.

Steps 1-3 should be undertaken immediately upon discovery of the breach. Step 4 should occur after the cause of the breach is identified to prevent future reoccurrences.

Did You Know...

Patient Complaints and the Media

Where a custodian is asked to comment on a patient complaint that has been brought to media attention, the custodian should advise the patient and the media that the custodian cannot comment publicly on the matter without explicit patient consent pursuant to the *PHIA*. This gives the patient the knowledge that if they want the matter to be openly discussed they first have to provide the custodian with consent. Consent should be in writing and should confirm the patient's acceptance of the risks of misuse of their information once it is discussed publicly.