# SAFEGUARD

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

VOLUME 3, ISSUE 1 MARCH, 2019



**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)


- Privacy Management Programs: OIPC Expectations
- Interacting with Applicants
- Informal Access to Information
- Correction of Personal Health Information
- Transfer of Custody or Control of Records


## OIPC REMINDERS AND UPDATES

### Training Reminder

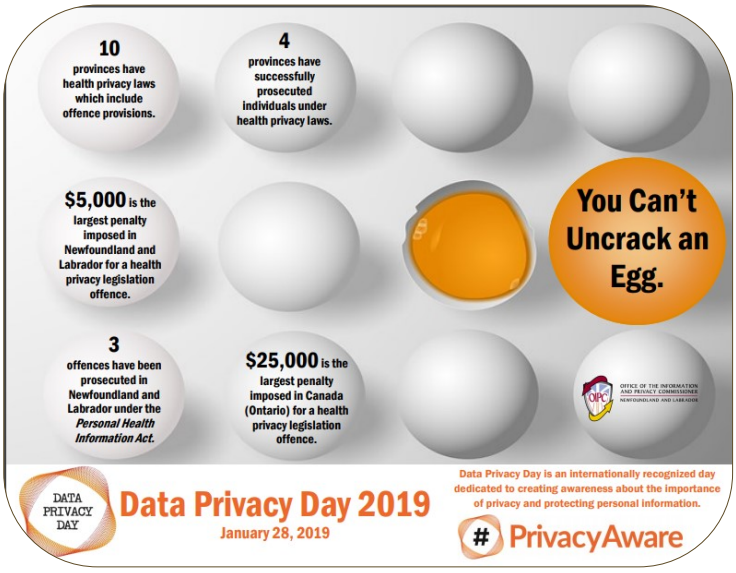
Did your staff have *PHIA* training in 2018?
If not, consider contacting our Office to arrange for training in 2019.
Also, consider whether you would like training about any specific access or privacy topic.

### Data Privacy Day 2019

Data Privacy Day (DPD) was January 28, 2019.

The OIPC created a poster in celebration of the event which is available on our website.

While DPD has passed, the message on the poster is still applicable and may be posted in your organization.



## PRIVACY MANAGEMENT PROGRAMS: OIPC EXPECTATIONS

The OIPC has been fielding many questions about our expectations with a Privacy Management Program (PMP). What is reasonable will vary based on such considerations as the volume of personal health information held, as well as the sensitivity of the information.

Some custodians will find it fairly easy to develop a PMP for a variety of reasons. Take, for example, a custodian that does not hold much personal health information (PHI), the PHI it does hold is not sensitive and the custodian enjoys a mature privacy culture. There is probably a PMP already in place, either formally or informally, so the gap analysis may reveal that much of the work required for a PMP is already complete. Compare this with a custodian that holds massive databases of PHI, much of it sensitive, with limited awareness of privacy. There will be much more work to be done to develop and document a PMP.

Any custodian that has PHI has legislative obligations under *PHIA*. Part of those obligations is to ensure reasonable safeguards are in place to protect PHI in its custody and control. One assumes that, the more sensitive the information, the greater the safeguards. This includes ensuring that appropriate privacy resources are in place to identify and address privacy concerns associated with the PHI. The custodian that holds large quantities of sensitive PHI should have more privacy resources in place than the custodian with little PHI.

When conducting a gap analysis, it is possible that a number of gaps will be identified, requiring the custodian to prioritize them. This Office would expect that gaps that represent high risks are addressed early in the PMP process, while low risk gaps may take longer. If a custodian identifies a number of high risk areas, it may need to dedicate additional resources to address them in a timely fashion.

The OIPC expectations will also consider the passage of time. These guidelines were released in March 2018. We do not expect custodians to be in compliance immediately. What we do expect is evidence of efforts towards compliance. We expect custodians to take the time to look at the guidance, understand how it impacts the organization, and take action to be in compliance. Our oversight approach allows more flexibility at the outset in circumstances where custodians face legitimate challenges and can document that best efforts are underway to bring the custodian into compliance.

While what is deemed reasonable may vary, what is certain is that the further out we are from the issue date of the PMP guidance document, the more this Office expects. Custodians that are subject of a privacy complaint or who submit a breach report can expect to be asked about the privacy tools it uses, such as PMPs and PIAs, on a go forward basis. Custodians that cannot demonstrate any effort to develop a PMP will be hard pressed to demonstrate compliance with *PHIA*.

We have also received calls regarding a template for a PMP. The PMP guidance document identifies the expectations of this Office and each custodian needs to determine what this will look like for them. As this will vary, this Office has no current plans to develop a template; there is no one template that will suit every custodian. That being said, various support tools are under development. Stay tuned....

## INTERACTING WITH APPLICANTS

As a custodian you will be called upon to interact with access to information applicants. Section 54 of *PHIA* mandates that custodians "offer assistance to the person requesting access" in order to ensure that sufficient details are provided by the applicant to allow you to identify and locate the records with reasonable effort. When an access request is received, the custodian should reach out to the applicant to ensure that the custodian has a clear understanding of what the applicant is requesting and seek any necessary clarity. In cases where there are other issues between the custodian and the applicant, these discussions may be uncomfortable but efforts should still be made. Be certain to keep records of all conversations with the applicant.

Following receipt of a Commissioner's Report, the public body is required to give notice of its decision in relation to the Commissioner's recommendations to the complainant. This notification is essential as it starts the applicant's appeal period should they wish to appeal the custodian's decision. Custodians should reach out to the complainant to advise that the decision has been sent and to ensure it has been received.

Interacting with Individuals Affected by Privacy Breaches

Finally, in relation to privacy breaches, custodians must be mindful that should notification of the breach be provided to affected individuals, that notification should include reference to the right of the individual to file a complaint with the OIPC. It should also provide the contact information for the OIPC. The OIPC breach notification form requires that you advise our Office if this reference was not included in the notification letter.

**PRACTICE TIP: Training & Awareness Activities**

Custodians should track all privacy training and awareness activities they offer. Having a record, including the topics covered and names of attendees, will assist when a custodian is called upon to demonstrate compliance with sections 13 and 14(3) of the *PHIA* following a privacy complaint or breach.

## INFORMAL ACCESS TO INFORMATION

Custodians are reminded that the *PHIA* does not prohibit informal access to information (i.e. access to PHI without completing a formal access request form). Section 59 of *PHIA* permits a custodian to release PHI to the individual that the information is about, so long as the disclosure is carried out in accordance with the *Act.* Should a custodian informally provide PHI to an individual, the individual will not be precluded from complaining to this Office should the information not be provided in accordance with the *Act* or should the individual believe that the information has not been fully provided.

Custodians should keep records of informal access requests, including the date on which the information was released; to whom it was released; a description of the records; and an indication and explanation of any records which were withheld.

# RESPONDING TO CORRECTION REQUESTS

A request for the correction of PHI may be made where the individual that the information is about believes the information is inaccurate or incomplete

Where such a request is made custodians have a legislative obligation to respond within 30 days. That timeframe can be extended if responding within the 30 days would unreasonably interfere with the operations of the custodian or if the information is so large a volume of records that the request cannot be completed within the 30 days. Any time a custodian extends the 30 day timeframe, the custodian must give notice of the extension to the requester and include the reason for the extension and the extended time period. Custodians must then respond within the extended time period. Failure to respond will be considered a refusal of the request and can be appealed to the OIPC or the Trial Division.

Granting a Correction Request

A correction request may be granted where the custodian is satisfied that the information is incomplete or inaccurate for its purposes and the applicant has provided the necessary information to allow the custodian to make the correction.

There are 3 methods for making a correction:

1. **Striking and Correcting**. Record the correct information in the record(s) and strike out the incorrect information but leave the information visible in the record.
2. **Severing, Linking and Correcting**: If striking the incorrect information from the record is not possible, the incorrect information should be severed from the record and placed in another separate record. At the location in the record where the information is severed, the severing should be labelled as incorrect information and a link leading to the incorrect information shall be placed in the document. The corrected information shall then be recorded either immediately before or after the severing with a clear indication that it is the corrected information.
3. **Direction**: If striking or severing are not possible and it is not possible to record the correct information in the record, the custodian must put a practical system in place to inform a person accessing the record that the information in the record is incorrect and to direct the person to the correct information.

Once a correction request is granted the custodian must notify the requester in writing that the request has been granted and the information has been corrected. The custodian must also provide written notice to anyone to whom the information has been disclosed within the 12 month period immediately prior to the request. The only exception is where the custodian reasonably believes that the correction will not have an impact on the ongoing provision of health care or other benefits to the requester or where the requester has advised that notice is not necessary.

Refusing a Correction Request

A correction request may be refused where:

- the custodian did not originally create the records and does not have the necessary knowledge, expertise and authority to correct the record; or

(continued on next page...)

## RESPONDING TO CORRECTION REQUESTS (CONT'D)

- the correction relates to a professional opinion or observation made in good faith; or
- the request is frivolous, vexatious or made in bad faith.

If a request is refused the custodian must make a note within the record of the exact wording of the requested correction and the fact that the request was refused. The custodian must also notify the requester in writing of the refusal, the reasons for the refusal, and the right of the requester to appeal the refusal to the Trial Division or the OIPC. The custodian must also provide written notice to anyone to whom the information has been disclosed within the 12 month period immediately prior to the request. The only exception to the latter is where the custodian reasonably believes that the correction will not have an impact on the ongoing provision of health care or other benefits to the requester or where the requester has advised that notice is not necessary.

## TRANSFER OF CUSTODY OR CONTROL OF RECORDS

A custodian has a legislative responsibility under *PHIA* to protect PHI. Unless or until a custodian passes custody or control to another custodian or dies without naming a successor custodian, this duty continues. A number of situations may arise where a custodian passes custody or control. The two most commonly encountered situations would be where a custodian retires or passes away.

Where a custodian passes away, and no succession planning has been done, the custodian's personal representative becomes responsible for and assumes the responsibilities of the deceased custodian until custody and control of the PHI passes to another custodian or person authorized under the *Act* to hold the PHI.

Where a custodian retires, prior to retiring the custodian should arrange for a successor to assume custody and control of the PHI following the custodian's retirement. The successor must be a custodian. If the successor is not a custodian and is, for example a storage company, the records have not been transferred and the retiring custodian maintains custody and control and the legislative obligations for the records. Where records are transferred to a successor, section 39 of *PHIA* requires the transferring custodian to make reasonable efforts to give notice to the individuals who are the subject of the information prior to the transfer or, where this is not possible, as soon as possible after the transfer that the transferring custodian has transferred the records. The notice should also identify and provide the contact information of the successor custodian and describe the means by which an individual whose PHI is involved in the transfer can access his or her record of PHI after the transfer. Notice can be done individually or by public notice; however, best practice would be to use both direct and indirect means of notification.

All transfers must be carried out in a secure manner using reasonable safeguards. What is reasonable will depend on the nature of the records (i.e. paper vs. electronic) and the sensitivity of the information.