Safeguard

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

VOLUME 1, ISSUE 3 NOVEMBER 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)

OIPC REMINDERS AND UPDATES

OIPC Website Now Searchable

The OIPC website, including Commissioner's Reports, is now searchable. The search field is located at the top of the "Commissioner's Reports" page under the "Reports" menu. Results include pdf documents such as: Commissioner's Reports, guidance documents, presentations, newsletters, and annual reports.

Material Privacy Breaches

Custodians are reminded that all material breaches must be reported to the OIPC. Section 5 of *PHIA* outlines the factors that are relevant in determining what constitutes a material breach, including the sensitivity of the information involved, the number of people involved, the potential for misuse of the information and whether there is a systemic problem. The OIPC is available to provide advice to custodians whenever they experience a breach. Breaches should be reported to the following email address: breachreport@oipc.nl.ca.

PHIA Review Complete

The conclusion of the statutory review of *PHIA* was announced on September 27, 2017. The review committee found that *PHIA* is not fundamentally flawed, but rather, needs some fine tuning. The recommendations represent potential improvements.

Next steps will entail careful consideration of all recommendations and amendments to the *Act* where appropriate. Amendments are anticipated to be brought to the House of Assembly in the fall of 2018. The committee's report is available at: PHIA Final Review Report.

Disclosure of Personal Health Information for Research Purposes

The legal framework surrounding the disclosure of PHI for research purposes is multi-faceted, and compliance with it is crucial in order to preserve and protect public trust in all health research efforts undertaken in the Province. A common understanding amongst stakeholders as to their respective duties to protect privacy is therefore essential. The *Health Research Ethics Authority Act* (*HREAA*) and *PHIA* address obligations of the Health Research Ethics Authority (HREA), custodians and researchers.

The HREA is empowered to ensure that health research involving human subjects is conducted in an ethical manner. This is achieved primarily via the requirement that all research in the Province involving human subjects be reviewed and approved by a Research Ethics Board (REB) established under the *HREAA*.

Although ethics approval by a REB takes privacy considerations into account, *PHIA* governs the privacy of PHI and imposes legal duties on researchers and custodians. Researchers and custodians must understand that HREA approval does not relieve them from their *PHIA* obligations related to the collection, use and disclosure of PHI.

Researchers should expect to have their REB approval documents reviewed by the custodian and be prepared that the custodian may have additional questions and/or place additional requirements on the project. These requirements may include: that the minimum amount of personal information is collected for the project; that it is accessed within the boundaries set by the custodian; and that it is stored securely, etc. Custodians should establish expectations regarding retention, destruction and future use, among other things.

Collecting and Disclosing Personal Health Information

There are two ways for a researcher to collect or access PHI under *PHIA*; both require REB approval.

1. Disclosure without Consent: PHI may be disclosed by a custodian without consent.
2. Collection with Consent: PHI may be collected with the consent of research subjects.

Where consent is required, section 23 of *PHIA* requires that consent be:

- of the individual the information is about;
- knowledgeable; and
- not obtained through deception and coercion.

Researchers cannot access information on the basis that such access is implied in the consent form to be necessary to accomplish the purpose of the research.

The OIPC will consider consent to be knowledgeable only if the sources of PHI are explicitly stated in the consent form and REB documentation. Details must also be provided as to how the information is being collected (directly or indirectly).

Cont'd...

Disclosure of Personal Health Information for Research Purposes (cont'd)

Researchers Obligations and Responsibilities

- Researchers must be explicit and identify in detail in their REB application the specific information they intend to access (or collect) from the custodian and/or the specific information they intend to collect directly from participants as part of the research project.

- Researchers who access or attempt to access PHI beyond what has been explicitly approved by the REB are accountable under *PHIA* and to the REB. Employers of researchers may also be held accountable if the research occurs in the course of employment by a custodian.

- If the scope of a research project changes after REB approval has been granted, it is the responsibility of the researcher to return to the REB to seek an amendment. Researchers need to update custodians if additional or expanded access to PHI is required.

Custodian Obligations and Responsibilities

- Custodians are accountable under *PHIA* when they permit access to the PHI of patients. Custodians should have an established review process for research requests that should, among other activities, ensure that the information being requested matches the information approved by the REB.

- When a custodian discloses information to a researcher, it does not transfer "ownership" of the data and the custodian should clearly establish expectations regarding retention, destruction and future use of data.

- If the custodian provides access to PHI beyond what has been explicitly approved by the REB, the disclosure is contrary to *PHIA* and the custodian is accountable for that disclosure. Similarly, it is not sufficient for *PHIA* compliance purposes to assert that a research proposal implies access to certain PHI.

- Custodians cannot rely on REB approval to satisfy their *PHIA* obligations. When considering a request from a researcher for access to PHI after REB approval, the decision whether to disclose the information is a discretionary decision by the custodian. Under *PHIA*, the custodian is accountable for the disclosure. The onus is therefore on the custodian to come to its own conclusion, after considering all relevant factors.

- Before the custodian grants access to a record of personal health information on the basis of consent, there is an onus on the custodian to review the consent to ensure that it meets the requirements of *PHIA*, including that the consent form be explicitly clear as to what information is intended to be accessed by the researcher.

Further details are included in the full guidance piece.

TRAVELLING WITH MOBILE DEVICES

Canada's Privacy Commissioner, Daniel Therrien has advised that U.S. Customs officers are entitled to look at mobile devices and even demand passwords under American law and unless you are unconcerned about U.S. officers accessing your mobile devices, you should not take them across the U.S. border.

If you are an employee of a public body and/or custodian and you are travelling with a device issued to you by your employer which has **personal information** and/or **personal health information** stored on it (or provides access to same) you have a legal obligation to protect the privacy of that information. Border officials may ignore claims of privacy and legal duties pursuant to the *ATIPPA, 2015* and/or *PHIA*. As such, you should carefully consider whether you might be risking exposure of personal information and/or personal health information to foreign government officials when crossing borders and take appropriate steps before travelling.

Public bodies and custodians are legally obliged to ensure that reasonable safeguards are in place to protect the privacy of personal information and/or personal health information. At a minimum, this requires policies regarding travelling while in possession of employer—issued mobile devices. Those policies should prohibit carrying personal information or personal health information on electronic devices while travelling. These policies must be communicated to all employees.

While both the *ATIPPA, 2015* and *PHIA* permit disclosures required by law, it is our position that this is limited to Canadian law and excludes knowingly creating the potential for disclosure of personal information and/or personal health information to foreign government officials.

For employees who use their personal devices to conduct the business of a public body and/or custodian the same considerations apply. Also, policies should cover both work and personal travel of employees. The practice of allowing employees to use their personal devices for business purposes, even with stringent safeguards, carries additional risks of unauthorized disclosure and further complicates crossing the U.S. border.

Our suggestions for measures that should be considered and included in travel policies and procedures and further details are included in the full guidance piece.

Avoiding the Risks of Ransomware

Yukon Commissioner Diane McLeod-McKay recently wrote an article providing tools for mitigating the risk of becoming a victim of a ransomware attack:

https://www.yukon-news.com/opinion/yukons-information-and-privacy-commissioner-how-medical-staff-can-avoid-the-risks-of-ransomware/

Custodians may find these tips helpful to implement in their own practice.

PRIVACY CHECKLIST FOR CUSTODIANS

PHIA requires that each custodian take steps that are **reasonable in the circumstances** to protect PHI in its custody or control. What is reasonable will depend on factors such as the sensitivity of the information, the degree of difficulty or cost associated with a particular security measure, etc. All safeguards should be periodically reassessed to ensure they remain effective and continue to meet the reasonableness standard set out in *PHIA*. This is particularly true for technical safeguards, given the rapid pace at which technology advances.

There are three (3) categories of safeguards which custodians should endeavor to put in place:

Administrative: written policies, procedures, standards and guidelines that protect PHI.

Technological: password use, encryption of mobile device, firewalls, and log-out timeouts.

Physical: locked filing cabinets, security alarms, keeping computer terminals and white boards away from public areas, and restricting access to unauthorized personnel.

A privacy breach is any collection, use or disclosure of PHI that is not authorized under *PHIA*. Breaches may be accidental or intentional. Most privacy breaches, unless the risk of harm is very low, must be reported to the affected individuals. More serious breaches must also be reported to the Commissioner. These are called material breaches. Section 5 of *PHIA* outlines the factors that are relevant in determining what constitutes a material breach.

Also, custodians are responsible for ensuring that employees, agents, contractors and volunteers are aware of their obligations under *PHIA* and of the custodian's *PHIA* policies and procedures.

Below is a quick checklist to help get you thinking about your obligations under *PHIA*. It should not be taken as a comprehensive or definitive guide on how to fulfill your responsibilities as a custodian.

Custodian Checklist

1. Do you have policies in place regarding PHI?
2. Do you have confidentiality agreements for employees, contractors and volunteers?
3. Are you employees aware of their obligations? Has there been privacy training?
4. Do you have reasonable physical security measures in place?
5. Do you have reasonable technical security measures in place?
6. Do you have reasonable administrative security measures in place?
7. Do you have a *PHIA* public written statement posted or provided?
8. How well do you inform your patients of their rights under *PHIA*?
9. How aware of you of what do in case of a privacy breach?

If you have any questions about meeting your obligations under *PHIA* please contact the OIPC.

Offence Charges under Personal Health Information Legislation

Since the proclamation of *PHIA* this office has laid charges against 3 individuals for snooping. Jurisdictions across the country have also laid charges under their respective health information legislation. In Alberta there have been 8 convictions under the *Health Information Act* and there is currently one other matter before the courts. In relation to the most recent conviction, the pharmacist received a conditional sentence of six months including three months of house arrest with some exceptions, to be followed by three months of a court-imposed curfew and also 20 hours of community service.

Recently in Manitoba, a former police officer and Manitoba Health employee, was found guilty of snooping into his relatives' health records. This was the first time the Manitoba Ombudsman filed charges under the *Personal Health Information Act*. The charge has a potential fine of $50,000; however, the court sentenced the man to a $7500 fine. The snooper was not identified to protect the identity of the relatives involved.

http://www.cbc.ca/news/canada/manitoba/manitoba-health-records-guilty-1.4142093

http://www.cbc.ca/news/canada/manitoba/phia-manitoba-health-employee-daughter-1.4303743

Educational & Training Opportunities

The OIPC is available to deliver training and educational seminars to all custodians. Presentations can provide a general *PHIA* overview or can be tailored to suit your needs and concerns.

To discuss possible topics or to make arrangements for presentations, please email: commissioner@oipc.nl.ca.

Access to or Correction of Personal Health Information

Patients have a right of access to their own PHI and a right to have errors in their PHI corrected. Both types of request must be made directly to the custodian in writing (or verbally, if for example, language is an issue). A request must contain sufficient information to allow the custodian to locate the records. If it does not, the custodian should assist the patient in clarifying their request.

Requests for access must responded to within 60 days. Requests for correction must be responded to within 30 days. Extensions are available in certain circumstances.

Section 58 sets out when a request for access must or may be refused. Where a request is refused, the patient may file a complaint with the Commissioner or proceed to Court. Section 62 sets out the permitted reasons for refusing to correct. Where a custodian refuses to make a correction, the custodian must make a note that a request for correction was filed and advise the patient why the correction was refused.