OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Submission of the
Office of the Information and Privacy Commissioner
to the *Personal Health Information Act*
Review Committee

February 13, 2017

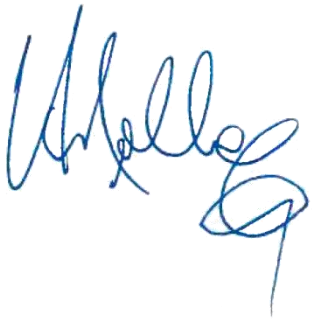
February 10, 2017

Mr. David Morgan
Chair
PHIA Review Committee

Dear Mr. Morgan,

I am pleased to provide to you and the Committee the submission of the Office of the Information and Privacy Commissioner in relation to the statutory review of the *Personal Health Information Act*, which was drafted by Sean Murray with contributions and input from other staff in the Office. Please do not hesitate to reach out to Mr. Murray should you or the Committee members require clarification on any items discussed in the submission or if you would like us to consider and provide comments on any aspect of *PHIA* that we have not already addressed.

Yours truly,



Information and Privacy Commissioner
Donovan Molloy, Q.C.

Table of Contents

Introduction

One very important provision in the *Personal Health Information Act* (*PHIA*) is the requirement that it be subject to a review every five years:

> *91. After the expiration of not more than 5 years after the coming into force of this Act or part of it and every 5 years after that, the minister shall refer it to a committee established by the minister for the purpose of undertaking a comprehensive review of the provisions and operation of this Act or part of it.*

With the continual march of technology, including electronic health records, advances in the use of genetic information, and the eventual ability of patients to access their own health records remotely via the internet, it is crucial that this law be reviewed regularly to ensure that it continues to serve its intended purposes. Although the review has been late in starting, we are pleased to see that it is underway and look forward to helping to improve *PHIA* in the interests of all citizens and stakeholders.

This Office has participated in two statutory reviews of the *Access to Information and Protection of Privacy Act* (*ATIPPA*), Newfoundland and Labrador's public sector access and privacy law. The first review was largely a closed-door affair which attracted relatively little public attention, although the resulting legislation, infamously known as Bill 29, certainly garnered a high profile because of the way it rolled back some positive aspects of the law which existed at the time. The second review was conducted by a panel of acknowledged experts with all of the resources necessary for it to set the gold standard in terms of review processes. The resulting law is the *ATIPPA, 2015*, which has been hailed by experts as the best of its kind in Canada and one of the best in the world.

Our challenge now is to aim high in terms of this legislative review of *PHIA*, both in process and outcome, but to do so without the level of resources available to the last *ATIPPA* review. We are off to a good start with a highly qualified and experienced review chair and committee supported by dedicated staff at the Department of Health and Community Services.

Similar to our submission to the *ATIPPA* review, this document will outline a few major themes for discussion as well as a number of specific recommendations which do not require a great deal of analysis. We would be pleased to provide further input to the Committee on anything in this submission, and to study and provide further input to the Committee on any topic of interest that we have not covered here. We also hope the Committee will consider recommending specific areas for policy development and education, even in areas where no amendment to *PHIA* is ultimately proposed. We look forward to participating in the review, and we hope that the final outcome will mean an improvement for privacy protection in the health sector for Newfoundlanders and Labradorians.

Oversight Model

It is our view that many of the flaws which existed in the *ATIPPA* oversight model prior to the *ATIPPA, 2015* are also present in *PHIA*. Ultimately, the problem is that there is no mechanism within *PHIA*, whether through the courts or through powers vested in the Commissioner, to compel compliance with the *Act* by custodians, except in relation to access and correction requests. In our 2014 submission to the *ATIPPA* review, we devoted significant space to presenting reasons why the ombuds-type, or recommendation-only oversight model was ineffective. As we noted in our submission, compliance with the law in place at the time was essentially voluntary, which is also the current circumstance under *PHIA*. That document beginning at page 69 contains a full discussion of the issues http://www.oipc.nl.ca/pdfs/OIPCSubmissionReviewofATIPPA2014.pdf

Although the *ATIPPA* Review Committee did not implement all of our specific recommendations, it fully endorsed the position taken by this Office about the need to improve the oversight model. In a sense, the Committee recognized the seriousness of the issues we had raised, but determined that we had not gone far enough in our proposed solution. Rather than simply building on the *ATIPPA* model that existed, which we had proposed, the Committee created and recommended a new oversight model, which has come to be known as the hybrid model.

The hybrid model is an approach which has been studied with interest by every other jurisdiction in Canada since its adoption here. As far as we know, jurisdictions which currently have order-making power are not proposing to switch to the hybrid model, however jurisdictions which currently operate under an ombuds model have spoken favourably about it.[1]

Ultimately, the issue is that the ombuds model is not as effective as either alternative, for the many reasons outlined in our submission to the *ATIPPA* review, noted above. The question remains, then, whether an order-making model or the hybrid model is to be preferred. In our case, we recommend adoption of the hybrid model for *PHIA*. We have had the benefit of using this model since June 2015, and we have found it to be extremely effective, significantly more so than the ombuds model for *ATIPPA*. It creates a motivation for public bodies to engage more fully with this

[1] Included among these is Daniel Therrien, Privacy Commissioner of Canada. In his letter of March 22, 2016, to the Standing Committee on Access to Information, Privacy and Ethics, in relation to the Committee's review of the federal *Privacy Act*, Commissioner Therrien recommended that the *Privacy Act* be amended to adopt the new hybrid oversight model recently enacted here in our *ATIPPA, 2015*. Following discussions with the federal Information Commissioner, Mr. Therrien later changed his position to align with the proposal of his colleague, Commissioner Legault, who had recommended order-making power for the Office of the Information Commissioner of Canada. It is our understanding that this change in position was a compromise in order to ensure that all of the federal institutions which are subject to both pieces of legislation would not have to deal with two oversight bodies with two different oversight models.

Office, because they know that the burden will be on them to go to court should they not wish to follow a recommendation of this Office. [2]

The primary benefit of the hybrid model over the order-making model, particularly for a smaller jurisdiction, is that it is simply an evolution of the ombuds model. Many of the processes of the ombuds model remain, except that in the end, a recommendation carries much more weight and consequence. With the order-making model, the informal resolution and investigatory processes must be completely and formally separated from the adjudication process. A separate adjudication unit would have to be established, including adjudicators who are separate from the investigative staff. Another element of the order-making model is the requirement for exchange of submissions and rebuttal, which adds significantly to the time consumed by the process.

A further benefit of the hybrid model is that the Commissioner retains a similar role vis-a-vis any future court appeals. The Commissioner may be a party or an intervenor on most matters which he has previously investigated under *ATIPPA, 2015*, because any subsequent court action is a trial *de novo* (a new matter), rather than an appeal of the Commissioner's decision. With order-making power, parties must appeal an order from the Commissioner, and the Commissioner therefore is more like a lower court whose ruling has been appealed to a higher court. Except in a narrow scope of procedural and jurisdictional issues, the Commissioner cannot become a party to such court proceedings. This means the Commissioner, who is often the only party with substantial experience in dealing with the *Act* and is certainly the only party with the sort of public interest perspective that an oversight body can bring, would be absent from the proceedings. This leaves the ordinary citizen to bear the entire burden themselves against the custodian, and if the citizen cannot afford legal representation, the Court may effectively only get one side of the argument. Based on past jurisprudence in this Province, courts have often availed of the Commissioner's participation in order to gather and absorb this unique, impartial expertise.

In the same section of our submission to the *ATIPPA* review panel, beginning on page 72, we also address other means of engaging in effective privacy oversight. Below we address several of these under the heading "Commissioner's Powers", including audit, privacy impact assessment, etc.

Appeals

Appeal by Commissioner

If our recommendation of a hybrid model is not accepted, we recommend in the alternative that section 73 (Commissioner's Report) should be amended in order to allow the Commissioner to

[2] Section 50(1) of *ATIPPA, 2015* specifies that all recommendations by the Commissioner that an applicant be granted access to information or that an individual's personal information be corrected is subject to this process. In terms of privacy complaints, only a recommendation under section 76(1) leads to the same process.

bring any matter resulting in a recommendation under 72(2)(c) and (d) to the Trial Division so as to seek enforcement of the recommendation if the custodian fails to or refuses to follow the Commissioner's recommendation. Currently any matters resulting in a recommendation under 72(2)(c) and (d) are entirely with the discretion of the custodian, resulting in the circumstance that all of the statutory requirements of custodians listed under those provisions are *de facto* voluntary standards with no means of enforcement attached to them.

An argument can be made that section 72(2)(a) and (b) have a greater association with an individual person pursuing individual rights. These provisions relate to reviews of administrative decisions regarding access or correction, and they are available to be pursued by an individual in the courts, providing the costs and procedures associated with proceeding in that way are not too daunting as to dissuade the attempt. In these cases, there is a clearly defined remedy available to the complainants, in that the Court may compel the custodian to grant access or correction. It is also noted that section 84 allows the Commissioner to pursue an appeal of a decision respecting 72(a) or (b) with the consent of the complainant. Ultimately, a clearly defined remedy is available to those individuals who wish to pursue it.

With respect to 72(2)(c) and (d), however, no such remedy is available. *PHIA* is not currently designed as a vehicle for recovery of damages for complainants. The primary value of recommendations under these provisions is forward-looking. The purpose of most recommendations under these provisions is associated with preventing future privacy breaches, and they do not provide a remedy to individual complainants. In some cases, privacy complainants wishing to "get their day in court" do not fully understand the limits of the available remedies under *PHIA*, and may pursue an appeal under (c) and (d) even when the remedies they may seek (discipline or termination of an employee, issuance of fines, recovery of damages, etc.) are simply not available through an appeal under *PHIA*.

That being said, it is important to ensure that a process is available to the Commissioner to be able to, when circumstances warrant, launch an appeal if recommendations under (c) and (d) are either refused or not followed by the custodian. This is very much in line with the Commissioner's public interest role in ensuring that privacy breaches are prevented where reasonably possible and that *PHIA* is viewed as a law, rather than a set of voluntary standards. The Commissioner is much better placed than a complainant to bring forward a case which is focused more on achieving future compliance than addressing past wrongs, and allowing the Commissioner to do so with respect to recommendations under (c) and (d) would accomplish this.

No Recommendations from Commissioner

The language in sections 73 and 74 should be amended to clarify that an appeal to Court by a complainant in relation to recommendations under 72(2)(a) or (b) should not be limited only to situations where the Commissioner does not make a recommendation. The reality is that sometimes

the Commissioner may make a recommendation, but it may not be sufficient from the point of view of the complainant to address his or her issues. The language in this section should be amended to read that the complainant clearly has a right to appeal to the Trial Division subsequent to issuance of the Report, *whether or not* the Commissioner issues a recommendation, as it relates to 72(2)(a) or (b). As noted above, an appeal should also be enabled for 72(2)(c) and (d), but only the Commissioner should be able to bring such an appeal. Sections 74 and 83 should be similarly amended. Section 54 of *ATIPPA, 2015* may be helpful as a reference.

Complementary Amendments

In order to remain consistent with our recommendations regarding sections 73 and 74, the following amendments to section 83 (Appeal by Individual) must be made:

- 83(1)(b)(ii): this must be changed to the effect of "the Commissioner has completed a Report and the custodian has issued a response or is deemed to have responded";
- 83(2)(b)(ii): this must reflect the notion that an appeal may be filed by the complainant following the issuance of the Commissioner's Report relating to a complaint under 66(1). Whether or not a recommendation was made by the Commissioner is immaterial.
- Section 83(4) should be amended to require that the Minister serve the Commissioner.

Section 85 (Conduct of Appeal) should be amended to indicate that the Trial Division should, at the request of a complainant, review the decision of a custodian that relates to a request for access or correction; however new language should be developed to either:

> a) accommodate appeals under a hybrid oversight model similar to the *ATIPPA, 2015* or
> b) accommodate an appeal by the Commissioner where the custodian refuses or fails to implement recommendations in a report under 72(1)(c) or (d).

Section 86 (Powers of Court on Appeal) should also be amended to incorporate either:

> a) the hybrid model which could see matters resulting from a Commissioner's report relating to section 72(c) or (d) coming before the court, or
> b) appeals brought by the Commissioner in relation to section 72(c) or (d). Section 86(a) should include an option to refer the decision back to the custodian for reconsideration in cases where the court determines that the exercise of discretion was not adequately considered, or was made in bad faith, or was made for a purpose other than the purpose for which the exception exists.

Commissioner's Powers

Audit

Section 95(1)(b) (General Powers and Duties) of *ATIPPA, 2015* provides the Commissioner with the authority to conduct audits. We recommend that this also be included in an amendment to section 79 of *PHIA*. In the course of carrying out our oversight function, we have often observed that some custodians have poor *PHIA* compliance in general. Rather than launch an investigation, we believe the appropriate tool to improve compliance is an audit. This will require an amendment, as noted, to section 79, but also a provision such as the one found at section 107 (Report) of *ATIPPA, 2015* in order to ensure that the audit can proceed effectively.

Although there may very well be appropriate subjects for audit at the Regional Health Authority level, one of the key areas where the audit tool would be most helpful is with respect to small custodians, for example, private physicians' offices. Based on anecdotal evidence, we are of the view that small independent custodians are furthest behind in terms of basic *PHIA* compliance, in comparison to Regional Health Authorities. Unlike with the Regional Health Authorities, however, the dispersed nature of the smaller custodians means that we have not had much direct contact with them, either in terms of our oversight role or even in terms of education and relationship-building.

In an effort to improve privacy compliance, the Office of the Information and Privacy Commissioner has reached out to physicians and offered a free, short "privacy check-up" in which we would, in the course of a 30 to 45 minute site visit, go through a checklist of questions and provide physicians with feedback on their privacy and security practices. The goal was to provide an opportunity to give constructive feedback to physicians outside of a formal investigative process, with no strings attached. No records of these meetings were to be kept by the OIPC for use in any future compliance exercises; it was entirely for the benefit of physicians who could see the value in participating. Unfortunately, despite receiving endorsement and support from the College of Physicians and Surgeons and the Newfoundland and Labrador Medical Association, no physicians took us up on this offer. As a result of this experience, we do not believe that voluntary measures are effective in allowing the OIPC to achieve oversight of small custodians. At the same time, simply waiting for complaints from the public is not an option, especially considering that individuals do not always know what privacy standards to expect, and even those patients who have privacy concerns may be reluctant to file a complaint against their own health care professionals / providers. Explicit audit authority, crafted in such a way that custodians must cooperate and facilitate the necessary site visits and interviews, is recommended.

Privacy Impact Assessment (PIA)

Currently, *PHIA* contains no requirements for a privacy impact assessment (PIA), while a number of other Canadian jurisdictions have incorporated this element into their equivalent statutes.[3] A PIA documents the information handling practices of an entity (in this case, a custodian) in relation to a project or initiative, describing the information collected, detailing who has access and what they can do with this access, outlining how the information flows and documenting the reason for the collection. All privacy risks of the project or system are identified, considered and documented in the PIA. This knowledge then allows one to assess what steps (i.e. mitigation activities) can reasonably be taken to protect the personal health information (PHI) held by the custodian. Reasonableness is the standard set out in section 15(1) (Security) of *PHIA*. Without such an assessment, it is very difficult to evaluate the reasonableness of proposed or existing safeguards, as reasonableness is relative to factors such as the sensitivity of PHI in the custodian's possession or control, the number of people who have access, the likelihood of a breach, and severity of the consequences of a breach. Therefore, a PIA is instrumental in protecting against breaches as well as in the event of a privacy breach investigation, as the mitigation activities decided upon and the reasons for these decisions are also documented in the PIA. This will become part of the analysis in determining whether there has been compliance with section 15 of *PHIA*.

We are cognizant that a requirement for all custodians to conduct PIAs may not be feasible here at this time. However, it is recommended that the Department of Health and Community Services, Workplace NL, the Provincial Public Health Laboratory, all Regional Health Authorities, the NL Centre for Health Information, as well as the faculties/schools of Memorial University which are custodians, be required to complete a privacy impact assessment with respect to all proposed new administrative practices and information systems or proposed upgrades/changes to existing practices and systems that relate to the collection, use, disclosure and storage of individually identifying health information (or information that could be reidentified), and submit same to the OIPC for review and comment prior to implementation of any changes. Some of these custodians are, in many cases, already conducting PIAs on various projects, and therefore the imposition of a legal requirement to do so should not be unduly onerous.

In the case of Memorial University, it is proposed that the PIA requirement for the relevant schools and faculties would **not** apply to research projects approved by a Research Ethics Board (REB), however it would apply to other undertakings by these custodians involving personal health information, such as research databases created by these schools and faculties, as an example.

[3] Examples of relevant comparable provisions include section 64 of Alberta's *Health Information Act*; section 15 of the Yukon *Health Information Act* Regulations; section 56 of New Brunswick's *Personal Health Information Privacy and Access Act;* section 89 of the Northwest Territories' *Health Information Act*.

The wording of a new PIA provision in *PHIA* should be clear and unambiguous and should expressly apply to both new systems and upgrades or modifications to existing systems. All PIAs should be submitted to the OIPC for review and comment prior to implementation of the changes (whether that be a completely new system or an upgrade or modification to an existing system). We note that this would contrast with the requirement regarding the submission of PIAs to the OIPC in the *ATIPPA, 2015* (wherein only PIAs regarding common or integrated programs or services must be submitted to the Commissioner in accordance with section 72, *ATIPPA, 2015*). Unfortunately, there have been differing interpretations surrounding the meaning of "common or integrated program or service" and thus there is confusion about when or if a PIA should be submitted to the OIPC for review. As a result, no PIAs have been provided for review to this Office by a public body in accordance with section 72, other than on a couple of occasions as a courtesy. In other words, when a PIA has been provided, it was made clear that doing so was not an acknowledgement that section 72 applied to the program or service, and it was only being provided as a courtesy. There is little value in a legislative provision which has no practical effect, so care should be taken to avoid this type of confusion in *PHIA*.

Compelling Production of Records from Non-Custodians

Sections 69, 70 and 71 address the Commissioner's power to compel production of records and to enter and inspect premises in conducting a review. However, these provisions only explicitly apply to custodians. Unfortunately, privacy breaches, by their very nature, are not strictly confined to custodians' premises. Without the express authority to require production we cannot always properly investigate a privacy breach nor can we act to demand that the non-custodian turn over the record or produce for inspection any record relevant to the breach investigation.

An authority to demand a non-custodian turn over a record allows the Commissioner to properly investigate a breach in which personal health information is faxed, mailed, emailed to or accessed electronically by a non-custodian. It allows us to intervene to contain a privacy breach and protect personal health information when the circumstances require it.

One example in which such authority would have been helpful was when health records were found on the ground in Grand Falls-Windsor, and the finder brought them to a local media outlet. The media outlet reported on the matter as a privacy breach but initially refused to return the records to the custodian. Eventually they were returned to the custodian after a written request from the Commissioner, however there are no remedies in *PHIA* available to either this Office or the custodian if the media outlet had refused.

We have also encountered this issue where an individual who applies for a job with a private employer is required to undergo tests to assess his or her fitness for work. The tests are commonly done by occupational health or physiotherapy clinics, and the prospective employee has signed a

consent authorizing the disclosure of the resulting assessment to the prospective employer or its agent. The tests commonly include drug use screening.

The problem arises when the employee is denied the position and asks for a copy of the assessment report in order to find out whether it contains errors. Our Office could compel production of the record from the custodian that conducted the assessment under existing provisions of *PHIA*, but often the custodian has not kept a copy of the report – all records having been sent to the employer. We have no power to compel production from a private, non-custodian employer.

It would therefore be useful if *PHIA* contained a provision to compel production of records relevant to an investigation from non-custodians. In addition, it would also be useful if *PHIA* contained a provision similar to *ATIPPA, 2015*, section 65, requiring that every custodian that creates a record containing personal health information of an individual, or discloses personal health information of an individual to a non-custodian, to retain that information for at least one year so that the individual has a reasonable opportunity to obtain access to it.

Section 88 of Alberta's *Health Information Act* contains a provision which says "the Commissioner may require any relevant record to be produced to the Commissioner and may examine any information in the record, whether or not the record is subject to the provisions of this Act."

It is recommended that *PHIA* be amended to provide this power to the Commissioner in circumstances where it is necessary for an investigation, or to contain a breach, or to prevent harm resulting from a privacy breach.

Sharing Information with Other Information and Privacy Commissioners

Patients in Newfoundland and Labrador are sometimes sent out of province for treatment not available here. It is important to ensure that the Commissioner can properly investigate a breach which spans more than one jurisdiction. This can only be done by providing the Commissioner with clear authority to work with counterparts in other jurisdictions. This authority exists in section 84 of Alberta's *Health Information Act* as well as in sections 36(1)(k) and (l) of British Columbia's *Personal Information Protection Act*.

It is recommended that *PHIA* be amended to include a provision allowing for the exchange of information with Commissioners from other Canadian jurisdictions for the purpose of coordinating activities in relation to the investigation of complaints involving two or more jurisdictions.

Own Motion Investigations

Section 73(3) of *ATIPPA, 2015* explicitly grants the Commissioner the authority to initiate an investigation on his or her own motion. Section 66(3) of *PHIA* says that an individual may file a

complaint respecting a contravention of *PHIA* regarding his or her own personal health information or that of another person. In practical terms, the *PHIA* provision has the effect of allowing the Commissioner to essentially commence an own motion investigation. If required, a person on the Commissioner's own staff can serve as complainant. It would, however, be clearer to maintain 66(3) as it is and to add an additional provision similar to 73(3) of *ATIPPA, 2015*.

Other Powers of Commissioner

Section 79 (Additional Powers) should be revised and enhanced where appropriate to establish greater consistency with the comparable provision in *ATIPPA, 2015*. It is proposed to add the following based on section 95(1)(a) of *ATIPPA, 2015*:

- conduct investigations to ensure compliance with this Act and the regulations;
- monitor and audit the practices and procedures employed by custodians in carrying out their responsibilities and duties under this Act;
- consult with any person with experience or expertise in any matter related to the purpose of this Act;
- inform the public from time to time of apparent deficiencies in the system, including the office of the commissioner; and
- take actions necessary to identify, promote, and where possible cause to be made adjustments to practices and procedures that will improve access to and protection of personal health information.

These provisions should also be accompanied by a provision comparable to section 95(3) of *ATIPPA, 2015* to ensure the necessary clarity regarding the commissioner's powers to undertake these activities.

Other Approaches to Better PHIA Compliance

In many respects there has been minimal compliance with certain aspects of *PHIA*, particularly by smaller custodians, including regulated health professionals in private practice. As noted above, we have attempted to address this by offering a short, no-strings-attached privacy check-up in the form of a site visit to physicians' offices, however this has received no uptake.

One option which could be explored is to make legislative or regulatory changes with the goal of making certain elements of *PHIA* compliance mandatory in order for health professionals to maintain their registration with their professional colleges or boards. For example, some health profession regulatory bodies have made completion of *PHIA* online training mandatory, and this has been positive. Alternatively, as discussed above, another approach would be to grant audit authority to the Commissioner and to ensure that the Commissioner can make enforceable

recommendations resulting from the audit. Additional resources would be required at the Commissioner's Office in order to carry out such an audit program.

We are quite open to suggestions as to how *PHIA* compliance can be encouraged for smaller custodians. In the past, this Office has made efforts to reach out to regulatory bodies and associations and offered to assist in developing policies and procedures, notice materials, etc, but we have gotten very little response. Ultimately, voluntary measures have not been effective. The law must be meaningful, otherwise we may continue with the present course, whereby it is seen as a low priority in some respects by smaller custodians.

Offence Provisions

Clarifying the Offence Threshold

In order to make the offence provision in *PHIA* as clear as it can be and to ensure that it covers all of the important parameters that it should address, the offence provision should be amended as follows:

- The language in 88(1)(a) should be changed to "obtains, uses, views, accesses, collects, discloses" and "without authorization or by falsely representing."
- 88(2) should include "alters, erases or destroys with the intent to evade a request for access or correction."

Limitation Period

This province is one of only three in Canada which has seen prosecutions and convictions for offences under legislation similar to *PHIA*. Although our primary efforts are associated with recommending best practices and helping custodians to avoid privacy breaches, there are times when a breach is intentional. We have encountered incidents where employees of custodians were aware that their actions were contrary to policy and contrary to *PHIA*, but chose to illegally access personal health information anyway. In such cases, prosecution is a tool available to ensure accountability and to uphold public confidence in the collection, use and disclosure of personal health information by custodians. It is hoped that publicity about prosecutions may also serve to deter others from intentionally breaching patient privacy.

One of the challenges for this Office in conducting an investigation for the purpose of recommending that the Attorney General consider initiating a prosecution is the time frame available for the investigation. Currently, *PHIA* is silent on this matter. As a result, section 7 of the *Provincial Offences Act* dictates the time frame, which provides for a limitation period of 12 months

from the day on which the matter arose. In other words, it is 12 months from the date the offence occurred.

It is our experience, as well as that of other jurisdictions where prosecutions have been undertaken, that they quite often involve electronic health records. Sometimes the offence is discovered through a related complaint, but a period of weeks, months, or years may have passed between the date of the occurrence and the date of discovery. This is often followed by an internal investigation by the custodian and a subsequent complaint to the Commissioner. This can pose a challenge and can indeed preclude pursuit of a prosecution. If you are assaulted, you know right away and can make a complaint to the police. If your privacy is breached, it may be some time before you become aware of it, even though the effect can be long-lasting and devastating. When we put this view forward to the *ATIPPA* review committee, based on our experience with two prosecutions, we recommended that the limitation period be expanded to 2 years from date of discovery. The Committee accepted our recommendation, and the new period is now found in section 115 of the *ATIPPA, 2015*. We believe it is necessary to adopt the same approach for *PHIA*.

Amount of Fine

Another consideration in relation to the offence provision is setting an appropriate amount for a fine. While education and training are clearly the highest priority in terms of preventing and discouraging activities contrary to *PHIA*, there are occasions when, despite knowing better, individuals have and will continue to wilfully violate *PHIA*. In the two convictions that have occurred under *PHIA*'s offence provision, the fines were $5000 and $1000. The maximum fine for an offence under *PHIA* is $10,000. As comparable statutes evolve, this is now considered to be on the low end. Ontario, for example, recently reviewed and amended its *PHIPA* to increase the maximum fine in section 72 to $100,000 for a natural person, and $500,000 for a party that is not a natural person (typically a corporation). Alberta's *Health Information Act*, in section 107, provides for a maximum fine for most offences of $50,000. There are some exceptional circumstances where the maximum fine is $100,000. While most fines imposed will never come close to the maximum, increasing the ceiling demonstrates to the court and the public that the Legislature regards the offence as a serious one.

While the *ATIPPA, 2015* has a maximum fine of $10,000, it should be observed that personal *health* information, which is covered by *PHIA*, is considered to be some of the most sensitive personal information available, more so typically than much of the information held by public bodies under *ATIPPA, 2015*. There must therefore be sufficient deterrent available to reflect this, so that individuals are less likely to be tempted to unlawfully access, use or disclose personal health information.

Many custodians are practicing health professionals in the private sector. While an employee of a custodian can sometimes receive other repercussions (depending on collective agreement rights and

HR policies), the health professional in private practice may not be subject to significant discipline for a breach of *PHIA*. In such cases, it is important for the court to be able to consider a greater range of penalty through increased fines. In some cases these individuals are well compensated, and a fine in the range of the ones which have been issued to date would likely not be of sufficient deterrent value. It is our recommendation that the maximum fine be increased to $50,000.

We also note that there are no penalties or consequences for a custodian or a person who violates section 89 (Non-retaliation). In order for this provision to be meaningful, there must be a penalty or consequence for violation. The OIPC are not labour relations experts, so we may not be the most appropriate agency to investigate such an allegation. The Committee may therefore wish to recommend whatever legislative amendments are required to the effect that such an investigation could be conducted under the auspices of the Labour Relations Board, similar to the process set out for investigating reprisals described in sections 21 to 23 of the *Public Interest Disclosure and Whistleblower Protection Act*. An appropriate penalty for the offence of retaliation should also be determined.

Home Care

Currently, section 4(1)(f) designates a health care provider as a custodian. Health care provider is a defined term in section 2(1)(k). The term "health care" is also broadly defined in section 2(1)(h). Depending on whether the care being provided meets the definition of health care, home support agencies would fall under this definition. As the agencies themselves would be custodians, their employees' activities are encompassed by *PHIA* whenever they are engaged in "health care". Generally speaking these agencies should have the capacity to develop policies and procedures and to ensure that their employees are appropriately trained.

On the other hand, there are individuals in the community who are not employed by home care agencies, but are employed directly by individuals requiring some level of care, or employed by the individual's family to perform the care. These individuals are not professionals as defined by the *Act*, and their employment may be long term or short term. There is no education standard, or even literacy standard, which must be attained by these workers in order to accept this employment. In many cases these individuals are performing various acts of health care, medication administration, accompanying clients to medical appointments, etc. On its face, these workers are custodians subject to *PHIA* when they are health care providers performing health care duties, yet it may not be realistic to expect that these individuals are aware of *PHIA*, or have the capacity to understand and comply with it. It is recommended therefore that private home support workers who are not employed by an agency be exempted from most of the requirements, roles and obligations of custodianship in *PHIA* except that they be subject to an overall confidentiality requirement as well as subject to the offence provisions. The only reasonable alternative to this is that they be removed from *PHIA* altogether.

Information Manager vs Custodian

Can one entity be a custodian in relation to one set of data and an information manager in relation to another? Certain large custodians are in such a position where they might also be viewed as information managers depending on the particular data in question. Section 4(2)(h) could be interpreted to disallow or at least discourage this. The *PHIA* Review process should examine, consider and consult as to whether *PHIA* should be clarified to allow a single entity to perform both roles in relation to different sets of data, and also to explore what implications, if any, such a change might have on the protection of the information.

As currently constituted, of course, any entity can only be recognized as an information manager when there is a custodian subject to *PHIA* which has contracted with the entity to serve as information manager. There is no basis in *PHIA* for a custodian to act as information manager for a non-custodian. Are there circumstances where a custodian has personal health information in its custody, but the information is being held by the custodian in an information manager role, yet the "owner" of the information is not a custodian subject to *PHIA*? Is the entity a custodian? Is there a need to recognize such circumstances in *PHIA*? We propose this topic for further discussion and consultation among stakeholders during this review.

Deceased Individuals - Section 7(e)

There has been some debate about this section, and a level of discomfort has been expressed by a couple of larger custodians about the breadth of authority and access to confidential personal health information associated with deceased individuals. This provision, while not unique in Canada, is not confined to the deceased person's "personal representative" as it is in some other jurisdictions. There has been some concern expressed that an estranged (although not divorced) spouse may have complete control, or another relative who in fact does not have a close relationship with the deceased may wield this authority.

Examples have been suggested that perhaps a deceased person who may have had an abortion or given up a child for adoption in the past, or had a sexually transmitted disease, may not want anyone, even a spouse or close relative, to know this information after they have passed on.

Serious consideration of all relevant implications must be given before amendment is contemplated. Some jurisdictions, such as Nova Scotia, New Brunswick and Ontario provide factors or considerations that a substitute-decision maker must apply when deciding whether to collect, use or disclose personal health information. We anticipate that custodians which have had direct experience with this provision will likely comment on this issue. We will review any such comments and may provide further input to the Committee at that time.

Breach Reporting and Notification - Section 15

A version of the terms in 15(3) should be added to section 15(4) to clarify it.

The OIPC is of the view that all breaches which attain the level of requiring notification to affected individuals should also be reported to the Commissioner. The additional effort on the part of custodians in doing so would be relatively minimal and the processes and forms are already in place because of the breach reporting standards in *ATIPPA, 2015*. The Commissioner's Office is satisfied, through experience with that *Act*, that this level of reporting will not unduly burden the Office's administration, and furthermore we have found it to be helpful in terms of monitoring compliance with *ATIPPA, 2015*, by helping us to identify and address issues which have arisen through breach reporting, and also in building a productive rapport with public bodies through the dialogue and consultation that often occurs as a result of breach reporting. We are also of the view that the threshold for breach reporting should be fully contained within this provision, rather than in the regulations.

In terms of notifying affected individuals, we believe that the status quo should be maintained with one addition. There should be a provision allowing the custodian to refrain from notifying an affected individual of a breach who would have otherwise been required to be notified where doing so "could reasonably be expected to result in a risk of serious harm to the mental or physical health or safety of the individual who is the subject of the information or another individual." This proposed wording is based on language in section 58(2)(d)(i). There should be a conditional requirement that a custodian that refrains from notifying an affected individual on the basis of such a provision must notify the Commissioner of that decision, and the Commissioner may recommend notification, as is currently the case under section 15(5).

Research and *PHIA*

Memorial University

In 2013, Patricia Kosseim, Senior General Counsel at the Office of the Privacy Commissioner of Canada, and Daryl Pullman, Associate Professor of Medical Ethics at Memorial University, along with other co-authors, published an article in the Journal of the American Medical Informatics Association which summarized and lauded the unique legislative regime which exists in this Province in relation to the governance of genetic research and privacy:

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3555321/

This article essentially concludes that a delicate balance has been struck which establishes an appropriate regime to facilitate important research while ensuring appropriate privacy protection. In

order for this balance to be maintained, it is essential that the Memorial University faculties and schools which employ the researchers be subject to *PHIA*. *PHIA* and the *Health Research Ethics Authority Act* (*HREA*) are designed to work together. There is no formal mechanism within *HREA* for a member of the public to complain about a privacy breach, and to have that allegation investigated and addressed through formal channels, which exists only through the Commissioner's Office where *PHIA* applies.

It is our understanding that Memorial University has made representations to government advocating for the removal or de-listing of the schools and faculties as custodians under *PHIA*. The value of the current model is predicated on the fact that the four schools/faculties at Memorial are custodians. It does not work as intended if they are not custodians. As explained by the authors, the fact that the researchers are affiliated with these faculties/schools means that the information they obtain for research purposes enjoys the protection of *PHIA*:

> *While PHIA allows exceptionally for the nonconsensual collection, use and disclosure of personal information for research upon approval by a REB in accordance with HREA, it does not exclude these activities from the scope of the Act altogether. PHIA would continue to govern the activities of the PTRG [Population Therapeutics Research Group] as a custodian under the Act, as well as the personal health information it holds. Hence, apart from PHIA's consent requirement from which HREA provides an exemption, other PHIA obligations to protect and secure personal health information, provide access rights thereto, notify in the event of breach, respond to complaints and submit to the review powers of the Information and Privacy Commissioner, persist as conditions for secondary research use of personal health information.*

In our experience, the interaction of *PHIA* and *HREA* is a precise and well-designed interaction of complementary statutes. This is a "made in Newfoundland and Labrador" model which other jurisdictions are studying closely. The removal of these particular custodians from *PHIA* will destroy that arrangement, and potentially lead to a number of negative outcomes.

We should bear in mind that a large proportion of research takes place using data for which no consent has been provided by the data subjects. The legislative framework which is currently in place is intended to protect the rights of those individuals, ensuring that their information is used appropriately while also ensuring the availability of such information for approved research projects. Ultimately there are many unanswered questions and many considerations regarding intended and unintended ramifications of such a proposed change.

Private Sector

An even greater challenge associated with ensuring effective oversight of privacy protection laws in relation to research data is that there are entities engaged in research activities in the private sector which are not subject to *PHIA* at all. While these firms would be subject to *PIPEDA*, there are many risks associated with private sector research which do not exist in the public sector. In the genetic research space, there have been instances in the past, including in this jurisdiction, but also in

Iceland and elsewhere, where private sector entities have removed personal health information of citizens from the jurisdiction, and such information may effectively be removed from the regulatory oversight or no longer subject to the laws of the jurisdiction in which it was collected, whether through sale of a company, bankruptcy, sale of assets, etc. In consideration of this Province's founder population and the interest it generates in the genetic research space, it is extremely important that government consider appropriate action to mitigate these risks before major research projects are approved. Because of the unique characteristics of this jurisdiction, there may be few if any legislative models available in order to ensure a reasonable level of protection.

Unless the province were to consider developing and enacting a private sector privacy statute which could be deemed substantially similar to *PIPEDA*, there may be difficulties in regulating private business within the constitutional regime which assigns powers and authorities to the provinces and the federal government. One option, which may partly address this situation, might involve adoption of a version of section 54 of Alberta's *Health Information Act*.

This provision requires custodians and researchers to enter into an agreement before the custodian is allowed to disclose the information. Section 54(4) says that if the researcher contravenes or fails to meet the terms and conditions of an agreement, the agreement is cancelled. Some of the elements of the agreement may duplicate what would likely be contained in an approval from the Research Ethics Board, but it provides some leverage to custodians in dealing with researchers who are non-custodians, and it places an onus on researchers to turn their minds to privacy legislation and the various elements of the agreement as specified in section 54. From an oversight perspective, it provides an additional entry point to the OIPC, in either auditing research agreements of custodians (contingent on audit power being assigned to the OIPC through amendment) or in accepting complaints from members of the public that a privacy breach has occurred, in contravention of a research agreement. It is arguable that such a provision need not apply to a researcher who is also a custodian, because oversight would already be available.

Challenges associated with privacy and research, particularly genetic research, are not unique to this jurisdiction, and there are no perfect solutions. It is important, therefore that we monitor efforts to grapple with these challenges in other jurisdictions. A recent development may be found in Australia, where a law is under consideration which would have the following effect:

> *Anyone who intentionally re-identifies a de-identified dataset from a federal agency could face two years' imprisonment, unless they work in a university or other state government body, or have a contract with the federal government that allows such work to be conducted.*

While we are not recommending this particular approach, we bring it to the Committee's attention as context for the discussion. The following links outline the rationale for and pitfalls of this approach:

http://www.zdnet.com/article/senate-introduces-legislation-criminalising-re-identification-of-anonymised-data/

http://www.zdnet.com/article/australian-data-re-identification-defendants-will-need-to-prove-their-innocence/

http://www.zdnet.com/article/agd-warned-proposed-data-re-identification-laws-could-kill-the-data-research-canary/

Direct to Consumer Genetic Testing

A final related issue we would like to bring to the attention of the *PHIA* Review Committee is associated with direct to consumer genetic testing. This is currently outside of the jurisdiction of *PHIA*, and we are not currently in a position to recommend a specific regulatory approach to address related privacy issues. In this context, the concern is not so much for provision of funds by the consumer to a company in exchange for genetic information, although there are concerns that this could drive unnecessary follow-up medical testing, concerns about the lack of genetic counselling, and concerns about the accuracy of the inferences and conclusions presented to consumers resulting from these tests. Beyond those, there is also a concern that genetic information gathered through these tests may be used for secondary purposes, including commercial and other research, beyond this jurisdiction and in fact anywhere in the world. The potential privacy implications are still evolving and may not be fully understood for many years, by which time the data will be long out of the control of affected individuals and beyond any regulatory reach within this Province or Canada. It is recommended that this area be subject to additional study, and a commitment by the Department of Health and Community Services to lead this study would be a welcome outcome of the *PHIA* review process. Essentially, the issues are of sufficient complexity and novelty, and we are not aware of any regulatory models from other jurisdictions which address this issue, that it is unlikely that the right approach can be arrived at in the short term. At the same time, given the Province's unique genetic resource, and the associated privacy risks, this issue should not be left to languish.

Ontario Bill 119 Amendments to *PHIPA*

It is generally acknowledged that, while there are significant differences, *PHIA* is largely modelled on Ontario's *PHIPA*. For that reason, it is important for the Review Committee to take note of the recent amendments to *PHIPA*, as that jurisdiction moves forward with "*PHIPA* 2.0". The recommendations below are not our only comments on Bill 119 - other recommendations based on Bill 119 amendments are found elsewhere in this submission, where they are better combined with related topics.

Defining "Use"

One of the most important amendments in Bill 119 is to the definition of "use" in section 2 of *PHIPA*. The current definition in *PHIA* focuses on use as a process where we "handle or deal with" the information. It can be argued from a practical standpoint, particularly given the rise of electronic health records, that handling or dealing with information necessarily includes simply viewing the record, because with a paper record, handling would likely go hand in hand with viewing. *PHIPA* ensures that this understanding of the concept of "use" is clear and explicit by amending the definition to state as follows: "use … means *to view*, handle or otherwise deal with" the information.

Such an amendment to *PHIA* would be consistent with our proposed amendment to section 88, where we have suggested that the term "view" be added to the offence provision. In both successful offence prosecutions which have been completed in this Province, the parties are known, through audit logs, to have viewed information that was outside of their job duties and that they did not have a legal right to access or view the information in question. Adding this level of specificity may assist custodians in clarifying the law to their employees, and hopefully help to prevent future offences.

Notifying Professional Colleges/Boards

Another new amendment to *PHIPA* is a requirement in section 17.1 that custodians must notify the professional regulatory body in cases where one of its members, who is an employee of the custodian,

1) is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee; or

2) resigns and the health information custodian has reasonable grounds to believe that the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

The provision also requires a custodian to notify professional regulatory bodies when:

1) a member's privileges are revoked, suspended or restricted as a result of the unauthorized collection, use, disclosure, retention or disposal of personal health information by the member; or

2) a member voluntarily relinquishes or voluntarily restricts his or her privileges with or affiliation with the custodian and the custodian has reasonable grounds to believe that this action is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention, or disposal of personal health information by the member.

The OIPC is of the view that this notification requirement may assist in better supporting privacy protection in the Province, but if the Committee is to consider such a requirement for *PHIA* it would be important to hear from stakeholders, including large and small professional colleges as well as the RHAs. Important questions would include: what impact such reporting might have on privacy protection as well as professional practice; whether such a requirement may deter custodians from reporting breaches or proceeding with an investigation in order to protect the member/employee; whether such reports are already being made in certain circumstances and what the impact has been; should RHAs/other custodians be required to report similar misuse of personal information of the Electronic Health Records (EHR) system (including the Electronic Medical Record (EMR)) to the Newfoundland and Labrador Centre for Health Information (NLCHI) so that access can be restricted?

Implementing *PHIA* Amendments

A key element of any effective legislative regime is implementation. After *PHIA* was passed by the legislature in 2008, it was decided that there must be a delay in proclamation in order to facilitate education of custodians and development of resources to assist those custodians in compliance with the *Act*. While a lot of time and effort was devoted to this task by all stakeholders, the results were mixed. For one, there was a three year gap until *PHIA* was proclaimed into force. That was unnecessarily long. Secondly, some of the resources, while well intentioned, have not been as useful as they could have been. This is simply a matter of hindsight, and we must learn from experience and try to improve.

One of the primary challenges has been *PHIA* compliance by small custodians. Resources must be re-developed with this audience in mind. Secondly, the *PHIA* on-line training, which has been very helpful, requires renewal. It will need to be updated to reflect changes in *PHIA* resulting from amendment, but the content also needs to be refreshed in order for it to retain its ongoing value. While the OIPC stands ready to participate fully in these processes, both will require a commitment from the Department of Health and Community Services, and the devotion of necessary resources. Whether this process will require any delay in proclamation depends on the substance of any amendments, but needless to say, any delay in proclamation should be a period of months rather than years.

Finally, it is important to recognize that any additional roles assigned to the Commissioner in order to improve *PHIA* compliance and make oversight effective must be accompanied by the resources necessary to carry out the work.

Table 1 – Small But Significant Items

Current *PHIA* Section	Suggested Changes
Duty to Assist on Access Request and Request for Correction – sections 54(2) and 63	Currently the duty to assist a person who is making an access request is limited to offering assistance in clarifying the scope of the request, and when a correction is requested, there is simply a duty to process the request for correction in a prescribed way without any positive obligation to assist. Section 13 of the *ATIPPA, 2015* is more robust and includes a duty to "make every reasonable effort to assist an applicant in making a request and to respond without delay to an applicant in an open, accurate and complete manner". Both sections 54(2) and 63 should be revised to reflect the *ATIPPA, 2015* duty to assist. The powers of the Commissioner in section 79 should also be enhanced to include bringing to the attention of the custodian a failure to fulfil the duty to assist, similar to section 95(2)(h) of the *ATIPPA, 2015*.
Definition of Custodian – section 4(1)(g)	This section includes a person who operates a health care facility, a licensed pharmacy, an ambulance service, or a centre, program or service for community health or mental health but does not clearly cover group practices. Greater clarity is needed around whether or not group practices are custodians in their own right. Consideration should also be given to providing examples along with the description in this provision. The legislation should be crafted in order to minimize the number of circumstances in which individuals or entities are confused as to whether or not they are custodians subject to *PHIA*.
Non-Custodians Becoming Custodians – sections 4(1)(m) and 4(5)	The definition of custodian includes non-custodians who become responsible for PHI due to bankruptcy or insolvency or when a custodian dies and all their duties and powers pass to their personal representative until it can be passed to another custodian. These two sections could be brought together given their common theme of non-custodians becoming custodians. As well, subsection 5 should be more explicitly temporary, and that parties gaining custodianship under 4(5) should only be required to keep the information secure and provide for access.

Donation of Body Part or Bodily Substance – section 5(1)(c)	The definition of personal health information includes: "the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance" This should be expanded to include non-donation collections such as testing, commercial or research purposes, as long as the sample is identifiable or reidentifiable. As data analytics continue to evolve, it seems likely that tissue samples will become more and more identifiable even when accompanied by less and less data about the individual. This is a subject area which the Committee should consider further. The OIPC Supplementary Submission to the 2014 *ATIPPA* Review contains and in-depth discussion on this subject in Appendix 2: http://www.oipc.nl.ca/pdfs/SupplementarySubmissionATIPPAReviewAugust2014.pdf
Obligations of Employers Regarding Students - section 14(1), (2) and (3)	A custodian who is an employer is required to ensure: an oath of confidentiality is signed; compliance with the *Act* and policies; and that employees, etc are aware of their duties under the *Act* and policies. These provisions should also reference students, in order to capture students in the health professions who may come in contact with personal health information during their training at health care facilities. The elements of the oath of confidentiality should be prescribed in the *PHIA* regulations to ensure that the oath effectively becomes a commitment by the individual not to do the things outlined in the offence provision.
Add Harm Test to Notice of Breach – section 15(7)	Currently no notice of a privacy breach is required where the custodian reasonably believes the breach will not have an adverse impact on the care or well-being of the individual. A custodian should also not be required to notify an affected individual where notification would result in a risk of serious harm to the mental or physical health or safety of the individual who is the subject of the information or another individual, as described in s.58(2)(d)(i) regarding refusing access.
Contact Person's Obligation - section 18(3)(b)	This section lists the people that the designated contact person must ensure are informed of their duties under *PHIA*. It should also reference students, in order to capture students in the health professions who may come in contact with personal health information during their training at health care facilities.

Information Manager Obligations - section 22	These obligations should be extended to agents and contractors whose role requires them to collect, use, disclose, maintain, destroy or otherwise interact with or handle personal health information.
Circle of Care – sections 24 and 25(1)	Section 24(2) appears to indicate that a "person" (such as a family member?) can be included in the circle of care, while 25(1)(a) appears to negate this. It is proposed that a family member may potentially be appropriately in the circle of care and the proposed amendment is intended to resolve this: Remove "notwithstanding s. 24(1)" from section 25(1) and add to 25(1)(a) and (b) "unless the person is within the circle of care under section 24."
Indirect Collection of Genetic Information – section 31(g)	This refers to the collection of personal health information which is family history or genetic information. It should be part of a wider analysis of the collection, use and disclosure of genetic information and whether this provision protects privacy sufficiently in the face of current or future demands.
Scope of Use of PHI – section 35	This section should not be limited to custodians. It should also include volunteers, contractors and students.
Clarity Needed Concerning Deceased Persons – Section 38	This section should be reviewed in conjunction with section 7 for clarity. We have been told by at least one Regional Health Authority in the past that they believe section 38 limits what can be disclosed to a personal representative of the deceased under section 7. This is an erroneous understanding of both provisions, however for the sake of clarity, any amendment to either should ensure that the meaning is clear. One way of doing this would be to delete section 38(c). Section 7(e) already allows the personal representative of the deceased to exercise any right or power of the deceased individual under *PHIA*. Section 38(c) may therefore be superfluous. The Committee should also consider if a specific provision is needed in order to allow a custodian to provide information to a person or an insurance company for the purpose of collecting on an insurance policy?
Disclosure to Registries – section 39(4)(d)	This section requires custodians to disclose PHI without consent to a "custodian designated in the regulations who compiles or maintains a registry of personal health information for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or bodily functions." Significant work by all stakeholders has gone into determining a process for designating a registry, including the OIPC, the Department of Health and Community Services, and Eastern Health. This process was finalized to the

	satisfaction of all parties in early 2016 and it was the understanding of the OIPC that Eastern Health would be designated to operate the Cancer Care Registry. It is our understanding that there are a number of other registries which are also awaiting designation. It is requested that this legislative review address the failure on the part of custodians and government to complete this process. The language of this provision should be changed such that each individual registry is required to be designated, as well as indicating which custodian will be responsible for the registry. The Commissioner's Office endorsed the process that was used to prepare the Cancer Care Registry for designation and there is now a template or model for a designation process in place to clearly define the purpose and scope of the registry as well as its operating parameters. Such a process is necessary considering that 39(4)(d) is a mandatory disclosure of personal health information without consent.
Disclosure for Enforcement Purposes – section 42(1)	This section requires disclosure without consent to an authorized "person carrying out an inspection, investigation or similar procedure". Either through policy, regulation or amendment, there should be a requirement that the custodian must take necessary steps necessary in the circumstances to be satisfied that there is a duly constituted inspection, investigation or similar procedure under *PHIA*, the *Child and Youth Care and Protection Act* or another federal or provincial statute.
Disclosure to Another Custodian to Detect or Prevent Fraud – section 42(2)	This section deals with other custodians but are there any provisions in *PHIA* which explicitly facilitate disclosure by a custodian to law enforcement where there is a reasonable expectation that the disclosure will detect or prevent fraud?
Disclosure of Registration Information – section 45	Currently reads disclosure "by the Minister". Would the Minister likely have custody or control of registration information? Should it be amended to read disclosure by NLCHI or MCP at the Minister's request or direction? Is MCP a separate custodian from DHCS? Is it assumed by *PHIA* that MCP is not a separate custodian? Should they be? How does this affect s. 45?

Time of Response to Access Request – section 55	The 60 day time limit for a response to an access request is longer than necessary. We recommend 30 days. Also s. 55(3) should contain a requirement that the individual be notified of his or her right to complain about a time extension to the Commissioner.
Fees – section 57	It should be stipulated either in the *Act* or regulations that a fee can only be charged for a record containing over a certain number of pages, say 50 or 100. Also, there should be a requirement that individuals be notified that they may file a complaint with the Commissioner about a fee.
Appeals – section 83	In order to remain consistent with our recommendations regarding sections 73 and 74, the following amendments to section 83 must be made: • 83(1)(b)(ii): this must be amended to the effect of "the Commissioner has completed a Report and the custodian has issued a response or is deemed to have responded"; • 83(2)(b)(ii): amend to reflect the notion that an appeal may be filed by the complainant following the issuance of the Commissioner's Report relating to a complaint under 66(1). Whether or not a recommendation was made by the Commissioner is immaterial. • Section 83(4) should be amended to require that the Minister serve the Commissioner.

Table 2 – Error Correction and Updating

Current *PHIA* Section	Suggested Changes
Error in section 4(2)(b)	There is an apparent typographical error – "a body with statutory responsibility for the discipline of health professionals" should read "health care professionals"
Definition of PHI and Genetic Information - section 5	The term "genetic information" could be explicitly included in the definition of personal health information so as to prevent any disagreement as to whether it is included.
Clarifying section 12(2) – the Intersection of *PHIA* and *ATIPPA, 2015*	The language in section 12(2) is not easy to decipher, although it is technically correct. From the point of view of user-friendliness, which will assist with application and interpretation by custodians, can 12(2) be expressed more simply?
Error in section 13(1)	Currently discusses disposition of "personal information" – this should read "personal health information".
Error in section 17	It currently reads "A custodian shall designate a person to make a decision required of a custodian under this Act." Amend by replacing with "a custodian which is not a natural person shall designate..."
Error in section 18(3)(c)	Change "inquires" to "inquiries."
Updating section 19(b)	Change terminology from "access information" to "contact information" – this is the more commonly understood term, and will avoid confusion with making a request for access.
Errors in section 31	Section 31(b) contains an error in construction – one solution may be to remove the second "it" in the sentence. Section 31(j) is unclear in terms of: 1. the types of parties from whom the information would be collected, 2. how this provision would typically be applied, and 3. why it is necessary.
Errors in section 34	34(m)(iii) "and" should be changed to "or"; 34(o) should be "or" not "and" at the end.
Clarity in section 39(1)(j)	The term "geographic area" may not be necessary and may unduly limit the application of this provision.

Clarity in section 39(3)(a)	Remove "within the jurisdiction" and replace with "of the personal information referred to in the notice." For example, an employer may change from one fitness-testing company to another one. The OHS/fitness testing personal health information may have to be transferred to the physician employed by the second company, but no one has ceased to be a custodian "within the jurisdiction."
Error in section 39(4)(e)	Change "and" to "or".
Response of the Custodian – section 56	It should be made clear that the right of appeal to the Commissioner or Trial Division includes a circumstance where the custodian takes the position that the record either does not exist or cannot be found.
Errors in sections 63(1)(c) and (2)(a)	"… preceding the request for correction unless" in both clauses should be changed to "preceding when the correction was made" and "preceding when the notation was made" respectively.
Producing Records to the Commissioner During an Investigation – section 69(3)	In light of the Supreme Court of Canada's recent decision respecting solicitor-client privilege, amend this provision to state "privilege under the law of evidence, *including solicitor-client privilege*" rather than just "privilege under the law of evidence" and/or add provisions to the effect of *ATIPPA, 2015*'s 97(5)(a) and 100(2).
Error and Update to section 79	79(c) should be amended to read "public and custodians" and replace "confidentiality" with "privacy."
Error in section 84(2)	Section 84(2) should be amended to replace "paragraph 83(1)(b)" with "under this Act."
Error and Update in section 85	85(2) should be amended to replace "public body" with "custodian." 85(3) should be amended to specifically reference "solicitor-client privilege" in light of the recent decision of the Supreme Court of Canada requiring more explicit statutory language. Ontario's Bill 119 amending *PHIPA* includes language in the equivalent provision – 72(7) of *PHIPA* – to address appropriate precautions during a prosecution of an offence. These should be adapted and incorporated here.
Errors in section 90	90(1)(l) should be amended to read designating a "registry" and indicating which custodian is to operate the registry. 90(1)(m) is intended to refer to section 45(3)(b) and needs to be amended.