



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

By Email

September 29, 2026

Personal Health Information Act Review Committee
Department of Health and Community Services
1st Floor, West Block, Confederation Building

Email: JanelleHippe@gov.nl.ca

Dear Ms. Hippe:

Subject: Submission of the Office of the Information and Privacy Commissioner (OIPC)

OIPC would like to provide the PHIA review committee with some materials that we hope are useful as the review of PHIA continues. It would have been the preference of this Office to provide more information, insights and expertise, but the timing of this review which coincides with the statutory review of the **Access to Information and Protection of Privacy Act, 2015** and the short timeline provided has not allowed that to occur. We have included in our materials a letter to the Deputy Minister dated September 18, 2026, outlining our concerns (Appendix “A”).

Given the lack of time to prepare new submissions regarding PHIA, this Office relies on our submissions for the PHIA review held in 2016 led by Dr. David Morgan (Appendix “B”) and in 2021 led by INQ Consulting (Appendix “C”). Many years later, the same challenges presented by this Office during those two reviews still exist today. Issues such as how custodians are defined and changing PHIA to match the hybrid role of the OIPC as set out in ATIPPA, 2015 are still prevalent and require amendment. Given the passage of time, new issues such as access to a minor’s digital health record, correction and annotation of medical records and the use of Artificial Intelligence (AI) in the healthcare context have arisen. We have attached for your review “The Right of Privacy for Minors – Medical Records” (Appendix “D”) and we also want to bring to the Committee’s attention our concerns regarding what we view as an emerging issue given the implementation of MyHealthNL and MyChartApp, which provide online access to health records. This Office has now issued two recent reports where an applicant has requested the correction of their health records. As more citizens start accessing their own medical information, disputes have arisen regarding what medical professionals document in the medical chart versus the patient’s recollection or impression of what occurred. We refer the review committee to our document “Correction and Annotation of Medical Charts Given the Accessibility of Charts by Patients in the Digital Age” at Appendix “E” for more information on this.

We have also attached the following, which we trust will be helpful to the Review Committee:

1. Privacy Complaint Report PI21-0000, McMaster University, dated February 28, 2024, from the Ontario Information and Privacy Commissioner (Appendix “F”); and
2. 2023 Position Statement from the Canadian Paediatric Society relating to considerations for privacy and confidentiality in adolescent health care service delivery (Appendix “G”).

We also have a Resolution of the Federal, Provincial and Territorial (FPT) Information and Privacy Commissioners adopted in September 2026 regarding Responsible Use of Artificial Intelligence in Health and Health Research which we can provide after the Quebec election is completed on October 5, 2026. We will require confirmation that the Review Committee will hold this document in confidence until the FPT Information and Privacy Commissioners release the resolution publicly, which will be after the British Columbia election on October 24, 2026.

Although we provided recommendations regarding AI in our 2023 PHIA review submissions, as you can appreciate there have been further developments since then that warrant additional comments. Paragraphs 66 and 132 to 155 of the report concerning McMaster University (referenced above), illustrate the difficulties that arise when there is no legislation regarding the use of AI. The Report also outlines the challenges that the Ontario Privacy Commissioner faced in not having appropriate legislation to enforce guardrails for the use of AI in that province by entities that are otherwise subject to her oversight.

Despite acknowledging the absence of statutory provisions to ensure the safe use of AI by public bodies, and therefore the lack of any statutory authority for her to do so, she proceeded to use her report to issue recommendations regarding the use of AI by public bodies. She did this, I believe, because privacy oversight is closely adjacent to the kinds of considerations that arise with the use of AI. While AI initiatives often involve the collection, use, and disclosure of personal health information, the potential impacts and harms, as well as the preventative steps and mitigations, are outside the scope of most privacy statutes. In this case, the Commissioner apparently concluded that there was simply no other body or authority available who could make these recommendations, and in the public interest, felt obligated to bring them forward. I believe her recommendations were well-considered and appropriate. That being said, given that we know the kinds of harms and risks that can arise from the use of AI, it is simply not appropriate that oversight be left to privacy commissioners or any other body without a clear mandate and legal authority to carry it out.

OIPC is in a unique position as a regulator to play an oversight role as AI is integrated into our healthcare system. With a broadened statutory mandate (as proposed in our previous PHIA submission) to consider not just privacy and access but other potential harms to society, OIPC can assist custodians in ensuring that AI is used for the primary benefit of our citizens by promoting measures that can help assess and avoid harms.

Legislative requirements for custodians to complete algorithmic impact assessments for any programs using AI with the ability of OIPC to conduct a review will assist in determining the risks, fairness and impacts of automatic decision making prior to going live. We reiterate that the scope of any OIPC review cannot only be privacy but must also include bias, discrimination or other flaws that can emerge through the way AI functions. Transparency and accountability will be necessary for the public to accept the use of AI and to prevent the plethora of harms that humans are becoming increasingly fearful of when discussing and using AI.

Social license is the term that is often used to describe the degree of public consensus or support behind an initiative. Public and private sector entities are clearly moving forward with AI implementation at speed, while it is unclear whether the social license yet exists for the intensity of change we are witnessing. It is, however, clear to anyone who reads the news that people around the world are clamouring for effective and appropriate regulation and oversight of AI. Through regulation and independent, effective oversight, public trust, and consequent social license, may actually be generated. In some larger jurisdictions, this may mean a separate AI statute and a new oversight model. Until that occurs here, OIPC, as an existing oversight office which already has an adjacent mandate would appear to be a ready option. Any non-independent entity that purports to perform an oversight function while operating within government may not receive the same level of public trust or credibility.

One small adjustment we would make to our submissions in 2020 about AI is that instead of notifying the Commissioner and requiring engagement on each use of AI, a published registry of AI impact assessments should be mandated, as is done by the federal government. The Commissioner should be entitled to require that a public body provide a particular AI impact assessment for review upon request, and the Commissioner should be enabled through clear statutory language to comment on any implications for the use of AI, such as those referenced by Ontario's Commissioner in her McMaster University report, or any other recommendations to mitigate any negative effects flowing from the use of AI, relating to or stemming from the collection, use, or disclosure of personal health information, that could have impacts on individuals, groups, or the public at large.

While this written submission is abbreviated given the short time that OIPC had to prepare, we encourage further consultation between OIPC and the Committee as it makes important recommendations about the future of PHIA. It is an essential component of this review that OIPC be provided with an opportunity to review and comment on the draft bill with ample time to provide our feedback prior to the bill being brought before the House of Assembly.

Yours truly,



Kerry Hatfield
Information and Privacy Commissioner

Attachments



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Personal Health Information Act Review

Submission of the
Information and Privacy Commissioner for
Newfoundland and Labrador

September 29, 2026

Table of Contents

OIPC PHIA Submission Appendices List

Appendix A	September 18, 2026, Letter to Deputy Minister of Health and Community Services Outlining OIPC Concerns with Time of Review
Appendix B-1	OIPC submission to the 2016 PHIA Review Committee
Appendix B-2	OIPC Supplementary Submission to the 2016 PHIA Review Committee
Appendix B-3	Further OIPC Comments to the 2016 PHIA Review Committee
Appendix C	OIPC Submission to the 2021 PHIA Review Committee
Appendix D	The Right of Privacy for Minors – Medical Records
Appendix E	Review of Correction and Annotation of Medical Charts Given the Accessibility of charts by patients in the digital age
Appendix F	Privacy Complaint Report PI21-00001, McMaster University, dated February 28, 2024, from the Ontario Information and Privacy Commissioner
Appendix G	2023 Position Statement from the Canadian Paediatric Society - Considerations for privacy and confidentiality in adolescent health care service delivery

Appendix A



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

September 18, 2026

VIA EMAIL

Tracy King
Deputy Minister
Department of Health and Community Services

Dear Ms. King:

Subject: PHIA Engagement Process

I am writing in relation to the **Personal Health Information Act** ("PHIA") engagement process recently announced by the Department of Health and Community Services. While this office commends the government's commitment to safeguarding personal health information, we must express our significant concern and disappointment regarding the timing and structure of this initiative. Specifically, we find the current approach problematic for these reasons:

1. **Lack of transparency and independence:** Unlike previous reviews of PHIA and ATIPPA, this engagement is not being conducted independently of the government, and we have seen no commitment that written submissions will be posted online for other stakeholders to see and respond to. Transparency of submissions is a key feature of reviews of this nature so that recommendations in written submissions can be questioned by other stakeholders or members of the public who may bring different expertise and experience. Such transparency would lead to a better result for all concerned and demonstrate the government's stated commitment to openness. Furthermore, characterizing this process as an "engagement" rather than a formal PHIA review – which is legislatively mandated under section 91 – is creating unnecessary confusion. If this is an engagement process only, will a PHIA review be completed subsequently as legislatively mandated?
2. **Conflicting time frames:** Conducting this engagement concurrently with the statutory review of the **Access to Information and Protection of Privacy Act, 2015** ("ATIPPA") places an impractical burden on key stakeholders. Some of the same entities operate within both frameworks. As the regulator for both pieces of legislation, our office is expected to provide substantive submissions and attend consultations for both processes simultaneously. Given the advocacy role played by my office on behalf of the people of the province, and

the fact that PHIA is a complex piece of legislation, we believe our role is crucial to ensure that the views of those who we hear from every day are reflected in this rights-based statute. Consequently, this overlapping timeline severely restricts the Office of the Information and Privacy Commissioner's ("OIPC") capacity to participate meaningfully, depriving the process of my office's insights and expertise.

3. **Insufficient Consultation Period:** The 30-day timeline is entirely inadequate. In all prior reviews, the OIPC has provided researched submissions and attended consultation meetings to ensure that the perspectives and concerns that we hear every day from residents of this province are thoroughly represented. As a small office, we cannot produce the quality and depth of submission required to address complex modern issues like parental access to children's health information and artificial intelligence within a restrictive 20 business day window.

In an era defined by digital health transformation and the integration of artificial intelligence, the government is correct to prioritize this legislation, which has not seen substantive amendment since it was passed in 2008. However, rushing to meet an accelerated fall timeline risks undermines the depth and quality of the review required before drafting new statutory language.

Therefore, we formally request that the deadline for written submissions and further stakeholder engagement be extended to early 2027, taking into account the current timelines established for the ATIPPA review. In the alternative, we formally request an opportunity to review and comment on the draft bill with ample time to review it and provide our feedback. As always, it is a pleasure to work with you and your team to ensure that personal health information of Newfoundlanders and Labradorians receives the best possible access and privacy protections.

Sincerely,



Kerry Hatfield
Information and Privacy Commissioner

Appendix B-1



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

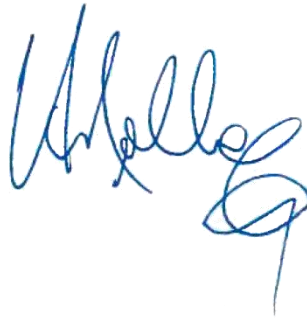
February 10, 2017

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,

A handwritten signature in blue ink, appearing to read 'Donovan Molloy', with a stylized flourish at the end.

Information and Privacy Commissioner
Donovan Molloy, Q.C.

Table of Contents

Introduction	1
Oversight Model.....	2
Appeals	3
<i>Appeal by Commissioner</i>	
<i>No Recommendations from Commissioner</i>	
<i>Complementary Amendments</i>	
Commissioner’s Powers	6
<i>Audit</i>	
<i>Privacy Impact Assessment (PIA)</i>	
<i>Compelling Production of Records from Non-Custodians</i>	
<i>Sharing Information with Other Information and Privacy Commissioners</i>	
<i>Own Motion Investigations</i>	
<i>Other Powers of Commissioner</i>	
<i>Other Approaches to Better PHIA Compliance</i>	
Offence Provisions	11
<i>Clarifying the Offence Threshold</i>	
<i>Limitation Period</i>	
<i>Amount of Fine</i>	
Home Care	13
Information Manager vs Custodian.....	14
Deceased Individuals – Section 7(e).....	14
Breach Reporting and Notification – Section 15.....	15
Research and PHIA	15
<i>Memorial University</i>	
<i>Private Sector</i>	
<i>Direct to Consumer Genetic Testing</i>	
Ontario Bill 119 Amendments to PHIPA.....	18
<i>Defining “Use”</i>	
<i>Notifying Professional Colleges/ Boards</i>	
Implementing PHIA Amendments	20
Table 1 – Small But Significant Items	21
Table 2 – Error Correction and Updating.....	26

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.ni.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 *PHLA*. In the course of carrying out our oversight function, we have often observed that some custodians have poor *PHLA* 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 *PHLA* 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 *PHLA*.

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 *PHLA*, there are occasions when, despite knowing better, individuals have and will continue to wilfully violate *PHLA*. In the two convictions that have occurred under *PHLA*'s offence provision, the fines were \$5000 and \$1000. The maximum fine for an offence under *PHLA* 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 *PHLA*, 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 *PHLA*. 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 *PHLA* 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 *PHLA* when they are health care providers performing health care duties, yet it may not be realistic to expect that these individuals are aware of *PHLA*, 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 *PHLA* 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 *PHLA* 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 <i>PHIA</i> 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 <i>ATIPPA, 2015</i> 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 <i>ATIPPA, 2015</i> 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 <i>ATIPPA, 2015</i>.
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 <i>PHIA</i>.
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 <i>ATIPPA</i> Review contains an 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 <i>Act</i> and policies; and that employees, etc are aware of their duties under the <i>Act</i> 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 <i>PHIA</i> 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 <i>PHIA</i>. 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 <i>PHIA</i>. 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 <i>PHIA</i>, the <i>Child and Youth Care and Protection Act</i> 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 <i>PHIA</i> 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 <i>PHIA</i> 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 <i>Act</i> 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 <i>PHLA</i> 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 <i>PHLA</i> and <i>ATIPPA</i> , 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, <i>including solicitor-client privilege</i> ” rather than just “privilege under the law of evidence” and/or add provisions to the effect of <i>ATIPPA, 2015</i> ’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 <i>PHIPA</i> includes language in the equivalent provision – 72(7) of <i>PHIPA</i> – 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.

Appendix B-2



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER

NEWFOUNDLAND AND LABRADOR

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

March 8, 2017

March 8, 2017

Dr. David Morgan
Chair
PHIA Review Committee

Dear Dr. Morgan:

I am pleased to provide you and the Committee with a supplementary submission from the Office of the Information and Privacy Commissioner in response to the Round 3 process of the statutory review of the *Personal Health Information Act*. As with our initial submission, it was drafted by Sean Murray with input from other staff in the Office. Once again, please do not hesitate to reach out to Mr. Murray should you or the Committee members require clarification on any items discussed in this submission or if you would like us to consider and provide further comments on any aspect of *PHIA*.

Yours truly,



Donovan Molloy, Q.C.
Information and Privacy Commissioner

Table of Contents

Introduction.....	1
Workplace NL.....	1
College of Massage Therapists (CMT).....	1
Eastern Health (EH)	2
Labrador-Grenfell Health (LG)	4
Newfoundland and Labrador Association of Social Workers (NLASW)	5
Central Health (CH)	6
Health Research Ethics Board (HREB)	7
Western Health.....	8
Newfoundland & Labrador Centre for Health Information (NLCHI).....	8
Sequence Bio	10
Newfoundland and Labrador Medical Association (NLMA)	11
Memorial University	12
Canadian Nurses Protective Society (CNPS).....	18

Introduction

According to the guidelines on the web site of the *PHLA* Review Committee, this opportunity to provide a supplementary submission allows stakeholders to respond to submissions made by others in the first round of the process. We will therefore proceed to list all of the submissions which were made in the first round and provide any comments we have in response to these submissions.

Workplace NL

We agree with the points brought forward in the Workplace NL submission.

College of Massage Therapists (CMT)

The CMT provided a brief submission, raising three points. The first is that “the definition of custodian does not specify if an RMT is self-employed who is the designated custodian.” In our view, *PHLA* is clear on this point. A self-employed Registered Massage Therapist (RMT) is a custodian by virtue of section 4(1)(e) combined with the definition of “health care professional” in section 2(1)(j)(viii).

The second point raised by CMT is more complex, and a practical one. It refers to the lack of clarity regarding custodianship in a multi-disciplinary practice involving multiple health professions. CMT states that *PHLA* provides no clear direction as to custodianship in such situations. This can become a particularly vexing question where patients are seeing more than one professional in the practice. In our initial submission to the *PHLA* Review Committee we referenced the fact that *PHLA* does not address group practices. We realize that it is possible for health professionals to determine the roles and relationships among health professionals regarding *PHLA* through agreements when setting up a practice. In our experience, this does not always occur, and the issue only comes to a head when accountability for information needs to be determined due to a breach or when one of the professionals wishes to leave the practice. At that point, when these issues were never considered in the past, it can be very difficult to sort things out. One perspective would be that it is up to custodians to understand and apply the law, and leave it at that. The problem, however, is that interpreting and applying *PHLA* can be difficult, and unless custodians are given clearer legislative provisions to follow, ultimately it may be patients who suffer when there is a failure to establish clear accountability. It would be helpful if the Committee could consider a better approach to defining custodianship which considers the different ways that health professionals set up their practices.

The third point raised by CMT is also worthy of consideration. There are circumstances in which the owner of a business which either employs health care professionals or rents space and provides facilities and amenities for health care professionals has asserted control over health records. *PHLA* does not allow a business owner who is not providing health care to patients to be the custodian. Rather it is the health professional who is the custodian, unless the operation falls within the unnecessarily vague and often misunderstood category in section 4(1)(g)(iv).

It is not always clear to CMT whether records of personal health information must stay with the business when an RMT departs, to potentially be passed onto another RMT who may come in as a replacement, or whether the RMT may take the information when he or she leaves, and thus

continue to be the custodian. Furthermore, the records involved might also be records relied upon by other custodians in the same location, such as chiropractors, physiotherapists, etc. As with the second question raised by CMT, if sufficient effort is put into establishing appropriate agreements up front, these questions can be managed within *PHIA* as it now stands, however this solution does not often reflect the practical realities encountered by CMT, and again it would be helpful if the Committee would consider whether an amendment to provide greater clarity might be feasible. Such an amendment might perhaps consider whether the definition of “custodian” should include “a person who operates a group practice of health care professionals”. Any such amendment should be undertaken bearing in mind the different operational arrangements in common use, ranging from situations where a health care professional is simply renting space in a building with other health care professionals, to situations where a business owner has hired health care professionals to work as employees, as well as other contractual arrangements. The outcome should be such that health care professionals and business owners enjoy greater clarity and encounter fewer difficulties determining who is intended by *PHIA* to serve as custodian.

Eastern Health (EH)

Eastern Health covered many topics in its submission, including the oath or affirmation. While we recognize the difficulties associated with an oath or affirmation for certain contractors, further consideration of this subject by the Committee may determine the most appropriate solution, or if any change is warranted at all. Further to EH’s comments, we are also of the view that the contents of the oath should be specified by regulation, and that the elements of the oath should reflect the language in the offence provision. Whether through policy or legislation, we would add the proposal that a new oath be required at specific intervals (perhaps every three years) and whenever an employee changes position.

In part C.3.1 of EH’s submission, there is a request for greater clarity as to the custodianship of information held in Meditech which was placed there by a physician who is also a custodian in his or her own right. It would seem that the physician should be considered the custodian, but of course it is EH which maintains the security of the system, and it is not possible for the physician to change it. Is EH then an information manager for the physician? These are important considerations when faced with questions as to whether EH or the physician has the right to make or is responsible for disclosures to researchers and others as permitted or required by *PHIA*. It is unclear whether this matter can be or should be resolved through written agreement between EH and physicians at the time access to Meditech is granted, or whether a legislative amendment is required. Further consideration of this issue by the Committee is warranted.

In part C.3.2 EH says that the definition of custodian must include those faculties and schools of post-secondary institutions which are involved in health research. This not only supports our position on the matter of ensuring that the parts of Memorial University which are currently custodians remain so, but opens the door for broadening the definition as well.

In part C.3.3, EH proposes that a separate category of custodianship which contains fewer disclosure provisions but many of the responsibilities of full custodianship be considered for private companies that are involved in the collection, use or disclosure of personal health information. Fundamentally this is the same issue that the OIPC and others have identified in terms of the problems associated with custodians disclosing personal health information to non-custodians,

usually in a research context, although there may be other contexts in the experience of EH. We don't explicitly endorse the proposed solution, but we recognize the concern. We have proposed a particular approach as have others, but the important thing is that the Committee is aware of this concern and that it make recommendations to remedy it.

In part C.6 EH expresses a need for a more prescriptive approach to fees. The recently revised, current policy regarding fees adopted by all RHAs seems fair and reasonable. It is not clear, however, whether this same policy is a good fit for all custodians. The OIPC released Report [AH-2012-001](#) on the subject in 2012. One newer issue which has emerged, however, relates to individual custodians who retire or cease to practice who contract with an out-of-province storage company to retain all the custodian's health records. We understand that the fees charged to patients for access by these companies can be excessive. Furthermore, if the practitioner remains a registered health professional in this province, the arrangement with the storage company would be an information manager arrangement. However, once the individual ceases to practice, or moves to another province or country, it is unclear whether the status of custodian still applies, and therefore whether there is any longer a valid information manager agreement, which requires a custodian to maintain such an agreement. We are hearing more and more of custodians utilizing the services of such companies, and it would be of great benefit to the public if *PHLA* would address this situation and ensure reasonable, affordable access to health records.

In part C.7 EH says that the 14 day time period for a custodian to produce a record to the Commissioner can be too restrictive. Section 24 of *ATIPPA, 2015* allows the Commissioner to consider extraordinary circumstances and to vary a time period under the *Act*. Perhaps a provision such as this may assist. A further point made by EH is that *PHLA* does not specify business versus calendar days. Central Health also raises this point. We have not seen this as a significant concern, however we do not oppose inclusion of a definition of "day" in *PHLA* as calendar days. Use of the "business day" approach can be confusing when the the definition of "holiday" in section 27(1)(l) of the *Interpretation Act* compares to the actual days when a custodian may be closed due to a recognized holiday. Furthermore, some custodians may routinely be open when a holiday as defined in the *Interpretation Act* occurs. This is compounded by the fact that some custodians operate in the private sector while others operate in the public sector, with variability between the recognized holidays. Again, we do not recommend a move to "business days" for *PHLA*, however if it would be helpful to custodians experiencing uncertainty, the term "day" in *PHLA* can be defined as calendar days.

In part C.8 EH recommends that there be a change in procedure specified in *PHLA*. Currently the custodian is required to notify the complainant of the custodian's decision in response to a recommendation in a Commissioner's Report. EH says that the complaint has been made to the Commissioner rather than the custodian, so the Commissioner should forward the custodian's response to the complainant. We have not heard of this being a significant issue in the past. It should be noted that the original complaint, which typically includes the complainant's address and other contact information, is required to be provided to the custodian by the Commissioner in accordance with section 66(5). If a circumstance were encountered by a custodian where there were difficulties in providing a response to a complainant, the Commissioner would be willing to assist where possible. We do not believe an amendment is warranted, and furthermore, any such amendment would be a break from the long established practice under *ATIPPA, 2015* which is common in other privacy statutes in Canada.

Labrador-Grenfell Health (LG)

LG proposes a definition of the term “spouse”. We agree that this would be helpful. LG also proposes that Regional Health Authorities (RHAs) be explicitly listed in section 24(2) for clarity. LG says that they believe RHAs are included because a health authority is a “person” in section 4(g) who operates a health care facility, however LG says that section 24(2) should be made explicitly clear to avoid confusion. The OIPC supports this recommendation, as it is important that *PHLA* be made as user-friendly as possible.

LG proposes greater clarity around the terms material breach, students, and deceased individuals, all of which we have addressed elsewhere. LG has also proposed that the terms “representative” and “personal representative” be clarified, which we support.

LG also requests clarification of the term “minor”, found in section 7(d). Central Health also makes a similar proposal. The current provision involves an assessment by the custodian as to whether the minor understands the nature of the right or power granted to him or her under *PHLA* and the consequences of exercising that right. LG proposes that a strict definition of the term “minor” be adopted, similar to the *Advance Health Care Directives Act*, in which a directive is presumed not valid if it is made by a person under the age of 16 and is presumed valid if the person is over 16. LG also references the *Children and Youth Care and Protection Act*, which defines a youth as a person between the ages of 16 and 18 and child as a person actually or apparently under the age of 16.

With no specific definition of “minor” in *PHLA*, the *Age of Majority Act* applies, which says that persons under the age of 19 are minors. For those patients, the custodian is required to make a determination as to what rights and powers of *PHLA* are available to the minor based on the circumstances, including the particular information and the capacity of the patient to understand it and the consequences of a decision he or she might make. The problem with the approach offered by LG is that it does not account for the ability of the individual or the context. Certain information may be able to be shared with a young patient, but other information may not because of its complexity and the capacity of the young person.

One of the issues which has been considered and discussed in significant depth at the Canada Health Infoway Privacy Forum is the age at which minors should be given access to their own personal health information through emerging technology often referred to as a patient portal. Significant research has been conducted on this subject, and it is important that we attempt to adopt an approach that considers new advances in the ways that patients interact with their own personal health information, such as patient portals, which could provide significant clinical value to all patients, including minors, depending on the circumstances. This may prove to be a valuable consideration in a Province with a large rural population and service delivery challenges.

Given the time available to prepare this submission, rather than repeat or try to summarize all of the research that has been conducted, several links are provided below to research papers, presentations and reports available on the Canada Health Infoway web site. These reports are quite recent and should be considered with some confidence to be among the latest work done on the subject in Canada. Canada Health Infoway provided permission for me to include links to these resources found on its web site, but has asked that the documents themselves not be republished on another web site or in other formats. We thank LG for raising this issue, and propose to the Committee that it be the subject of greater in-depth study.

<https://www.infoway-inforoute.ca/en/what-we-do/blog/consumer-health/7233-what-canadians-think-about-adolescents-accessing-their-electronic-personal-health-information>

<https://www.infoway-inforoute.ca/en/what-we-do/blog/consumer-health/7195-adolescent-access-to-digital-health-records-results-of-an-environmental-scan>

<https://www.infoway-inforoute.ca/en/component/edocman/webinars-en/3130-webinar-pandora-s-box-is-open-mature-minors-access-to-their-health-information?Itemid=101>

<https://www.infoway-inforoute.ca/en/component/edocman/resources/reports/3118-pandora-s-box-adolescent-access-to-digital-health-records-research-summary?Itemid=101>

<https://www.infoway-inforoute.ca/en/component/edocman/resources/3088-adolescent-e-access-research-final-report?Itemid=101>

<https://www.infoway-inforoute.ca/en/component/edocman/resources/3087-provisions-relating-to-minors-in-provincial-and-territorial-health-information-privacy-and-health-care-consent-statutes?Itemid=101>

<https://www.infoway-inforoute.ca/en/component/edocman/resources/3085-environmental-scan-statutory-provisions-relating-to-rights-of-minors-summary-table?Itemid=101>

<https://www.infoway-inforoute.ca/en/component/edocman/resources/3083-environmental-scan-statutory-provisions-relating-to-rights-of-minors?Itemid=101>

<https://www.infoway-inforoute.ca/en/component/edocman/resources/3081-environmental-scan-processes-to-enable-adolescent-access-to-personal-health-records?Itemid=101>

Newfoundland and Labrador Association of Social Workers (NLASW)

NLASW filed a brief submission which identifies several topics of interest, some of which we have addressed elsewhere. One of the recommendations of NLASW is that “ongoing education pertaining to *PHIA* through the privacy office is recommended.” It is unclear if this is meant to refer to the Commissioner or the privacy office at the Department of Health and Community Services. Speaking for the Commissioner’s Office, we are ready at the invitation of any professional body, custodian or group of custodians to address any particular topic, or to work with them to assist in the delivery of education on a broad array of topics related to *PHIA*.

It must be observed, however, that section 14(2) places this onus on custodians to a large degree. While the Commissioner has a specific duty to inform the public about the *Act* in accordance with section 79, and it is agreed that this is something we need to pursue with greater vigor, there is a reason why custodians must take on their own education role as required by *PHIA*. Essentially, *PHIA* relies to a significant degree on the requirement that custodians develop their own policies and procedures in compliance with *PHIA*, and the rationale for this is that each custodian operates in his or her own field of professional expertise (or multiple fields), and ways of doing things may vary across specialties and be dependent on the size of the custodian organization. The training/education component then must be partly based on *PHIA* itself and partly based on the particular policies and procedures of each custodian. The OIPC is certainly available as a resource to

discuss the essential elements of such policies and procedures, to review drafts and provide input, etc, but *PHLA* rests on the assumption that this work, and subsequent education about *PHLA* and the policies and procedures, is the responsibility of the custodian.

NLASW proposes some additional points of clarification which are worthy of consideration, such as incorporating electronic communication (texts, e-mails, etc) within the definition of the types of records which can contain personal health information. NLASW also proposes that the term “guardian” be defined, which we support for the benefit of greater clarity and understanding.

Central Health (CH)

Central Health provided a number of suggestions, recommendations and comments. First among them is the recommendation that the term “agent” be better clarified through a revised definition. This has come up elsewhere and we support this recommendation.

CH also proposed that home support agencies should be included as custodians under *PHLA*. We believe that home support agencies are *already* custodians in accordance with 4(1)(g)(iv) as a “person” who operates a program or service for community health, the primary purpose of which is the provision of health care by a health care provider. The terms “person”, “health care provider” and “health care” are defined in *PHLA*. The definition of health care includes “care ... [for the] promotion of health.” That being said, we accept that there should be greater clarity and that home support agencies should be included explicitly as custodians in order to make *PHLA* more user-friendly. Generally speaking, it should not require an in-depth legislative interpretation to determine whether home support agencies, which play a significant role in health care, are custodians or not, and this can be resolved through the amendment proposed by CH.

CH discusses the issue of the rights of minors, however we have addressed that issue elsewhere in this document with respect to the submission of Labrador-Grenfell.

CH discusses section 6(2)(c) which states that even where a custodian is permitted to disclose personal health information without the consent of the individual, there is no prohibition against seeking the consent of the individual before disclosing. CH asserts that this provision may result in an interpretation in the minds of some health professionals who have a statutory obligation to report, such as under the *Children and Youth Care and Protection Act*, that there may be a resultant risk of harm if they seek consent first. The important distinction here is between the terms “permits” and “requires”. This provision refers to situations where a disclosure is permitted rather than required. Section 6(2)(c) would not apply to any disclosures without consent that are required rather than permitted. In other words, any disclosure that is mandatory (rather than merely permitted) is not subject to section 6(2)(c).

CH also raises an interesting issue with respect to section 41(2)(a) in which a custodian “may disclose personal health information for the purpose of a proceeding or contemplated proceeding in which the custodian is or is expected to be a party or a witness where the information relates to or is a matter in issue in the proceeding or contemplated proceeding.” CH questions whether there is authority in this provision to disclose to a disciplinary body of a health care profession in certain circumstances. This point deserves investigation and further consideration.

CH also discusses section 42 – disclosure for enforcement purposes, and raises a number of interesting points. CH refers to differences in the analogous provision in Ontario’s *Personal Health Information Protection Act (PHIPA)*. Although the OIPC’s initial submission to the *PHIA* Review Committee recommended some changes to this provision, the points made by CH also deserve further consideration.

CH offers some useful commentary on section 7 with respect to the person who can act in the place of a deceased person. While the term “personal representative” is a term with broad application in law and is understood as having a specific meaning, there is value in defining it in *PHIA* in order to make the *Act* more user-friendly. The primary issue brought to light by CH though is the fact that the term spouse as found in the *Advance Health Care Directives Act* does not include a non-married but cohabiting partner. CH points out other provincial legislation which does include this broader definition, but also points out that custodians are currently limited by section 7(e) to only considering the nearest relative as determined by the *Advance Health Care Directives Act*. This has been problematic on a practical level, and should be addressed through amendment.

Health Research Ethics Board (HREB)

Both HREB and the Newfoundland and Labrador Centre for Health Information (NLCHI) have proposed reviewing the differences in the definition of research in *PHIA* as compared to *HREA* and potentially amending one of them to make them consistent. As with our comments on NLCHI’s recommendation, the OIPC is of the view that these *Acts* have different purposes, and it is not clear that a change is warranted to *PHIA*. However, if any amendment is contemplated to *PHIA*, we believe there should be a more in-depth discussion and investigation of the potential impacts.

That being said, HREB has noted that there are research activities that are exempt from Research Ethics Board (REB) review, and that the *PHIA* review committee may wish to “evaluate the current governance environment of research activities that are exempt from REB review that rely on the use or disclosure of personal health information.” We support this recommendation.

HREB also proposes that certain other non-research activities which are exempt from REB review, including quality assurance and quality improvement studies, program evaluation activities and performance reviews, be subject to scrutiny by the Committee given the potential ethical considerations associated with these activities. We support this recommendation. If the Committee intends to investigate this area, they may wish to review Bill 70, currently before the House of Assembly, which introduces a new *Patient Safety Act*.

HREB also proposes that the treatment of non-health research that uses personal health information should also be examined by the Committee. We support this recommendation.

HREB also proposes that the Committee examine whether additional clarity is needed in circumstances where custodians receive a request to disclose data but there is some difficulty in determining who the receiving custodian will be, and thus who is accountable for data after it is disclosed. This may arise in situations where it is unclear whether the individual making the request or the organization associated with the individual will ultimately be the custodian under *PHIA*. Clearly, it is essential that custodians in receipt of a request to disclose data must establish whether

the intended recipient is also a custodian under *PHIA* in order to establish what can be expected of the receiving party and where accountability for the information lies. Whether this is something that must be addressed through legislation or policy is an open question.

HREB also raises the question of ongoing governance of personal health information after it has been disclosed to a non-custodian for research purposes and questions whether *PHIA* is currently adequate to clearly address this. In our view this question is tied to the issue we raised regarding disclosure of information for research purposes to non-custodians, which has been echoed in other submissions. We believe this is a very important question to be resolved in this Review.

HREB goes on to discuss in detail issues associated with the application of section 44, generally concluding that this provision is not adequate to handle issues around the disclosure of personal health information for research purposes. Included among the points raised by HREB is that REB approval does not absolve custodians of their responsibility to consider whether disclosure should or should not occur, and that *PHIA* should address the responsibilities of custodians in that regard. HREB has raised a number salient points which deserve careful consideration and we support the comments and recommendations presented by HREB.

Western Health

Western Health provides useful commentary and recommendations on the terms “student”, “spouse”, “minor”, “material breach” and on the subjects of deceased individuals and the status of Regional Health Authorities under section 24. We have addressed all of these issues either in our initial submission or in this document in response to similar comments and recommendations made by other stakeholders.

Newfoundland & Labrador Centre for Health Information (NLCHI)

NLCHI covered a wide range of topics in its submission. The first one raised was the suggestion that the term “information network” be clarified and that the process for designation be spelled out in the regulations. We have no objection to this suggestion. Later in its submission on page 5, NLCHI provides further support for its position with reference to the regime for designating an information network which is specified by law in Alberta and Ontario. NLCHI advocates that such a provision be created here in order to facilitate greater transparency and public awareness. We support this proposal.

NLCHI proposes that the term “research” in *PHIA* should align with the one found in *HREA* for consistency. The differences in the definition were also noted by the HREB. It is not clear whether the *HREA* definition would be the one to change or the one in *PHIA*. Adjusting the definition in *PHIA* could have significant impacts, perhaps unintended ones, and we would not recommend it unless there were an opportunity for a much more fulsome discussion on the implications.

We agree with the suggestion by NLCHI that additional clarification would be helpful regarding the term “evaluation.”

NLCHI has proposed that the term “person” be defined. We believe the term is appropriately defined in section 2(1)(o).

NLCHI proposes that “genetic information” should be explicitly included in the definition of personal health information. We support this recommendation.

NLCHI’s comments with regard to registries created under section 39(4)(d) are consistent with those raised in the OIPC submission. NLCHI proposes that a process for designating a registry be spelled out in *PHIA* or in the Regulations. This Office, along with the Department of Health and Community Services, has invested a significant amount of time in working towards a viable process for doing so, and we would be pleased to see it reflected in the regulations.

It must be observed that, currently, any registries operating in the Province are operating in non-compliance with *PHIA* and thus are in violation of the law, because none have been formally designated by regulation. It was expected after initial proclamation of *PHIA* that all registries would be appropriately designated within a reasonable period of time, however this did not occur. This state of affairs regarding registries cannot be allowed to continue. The current process must be formalized, and registries must be designated.

Of crucial importance is that there must be a process for either the Minister or the Commissioner (as is the case in Ontario) to review, at defined intervals, the operation of each registry, to ensure that it continues to operate as intended, and that if there is to be any expansion of the mission or function of a registry, that any such proposed new mandate be subject to appropriate scrutiny from a privacy perspective. The fact that registries amass a huge amount of personal health information on a mandatory basis without consent must not be forgotten in the course of moving forward with the laudable public health goals facilitated by registries.

NLCHI makes a number of important points in relation to disclosure for research purposes in accordance with section 44. NLCHI would like to see this provision expanded to include specific parameters. Other submissions, including the initial OIPC submission, have proposed something similar, although not identical. There seems to be consensus among many stakeholders that clear parameters and criteria are appropriate and would add significant value to the process.

As we note elsewhere in this submission with regard to the recommendation of Memorial University that its schools/faculties be de-listed as custodians under *PHIA*, NLCHI also underscores the potential negative impact on researchers and their ability to acquire data necessary to proceed with their projects if such custodians were de-listed.

NLCHI notes that organizations which de-identify personal health information yet retain the code which could be used to re-identify it are considered to hold identifiable information. We would agree. The Centre notes that it considers all record-level data to be identifiable due to the small population size in this Province, and the fact that de-identified information could in many cases be re-identified. NLCHI is of the view that de-identification and re-identification are not understood and applied consistently across custodians, and therefore advocates that *PHIA* be amended to resolve this. NLCHI further supports inclusion of a definition of “aggregate” information as found in Alberta’s HIA. We support these positions.

NLCHI proposes additional clarity regarding how privacy should be handled for the aboriginal community. No specific concerns were referenced by NLCHI but we would support further consideration of this issue.

Comments by NLCHI about the role of information manager in *PHLA* are consistent with those presented by this Office, however consideration should also be given to situations where NLCHI is in a role which would appear to be that of information manager but NLCHI is managing information of a non-custodian. Unless subject to an amendment, it is not possible for NLCHI to assume the role of information manager in such a situation, and by default it would have to be acting as a custodian.

Sequence Bio

It is important to recognize at the outset that Sequence Bio will very likely not be the only company to come forward within this Province to propose genetic research as a business undertaking. The approach taken by the *PHLA* Review Committee and ultimately the Government of Newfoundland and Labrador to determine what if any legislative changes will be made to *PHLA* will likely determine whether such undertakings can be accomplished in a way that provides sufficient value to the citizens of the province to justify any social or economic costs or risks. The process of determining the potential value and the costs or risks is one that should be subject to significant research and analysis. Is the value real – does it live up to the hype? Can we even predict the potential value at this point? What are the costs and risks – how well are they understood? Are they exaggerated? Are there too many “unknown unknowns” at this point? Beyond Sequence Bio, there remain larger questions about how we apply basic privacy principles to genetic research, for example, how can one individual consent to participate in a research study which necessarily involves the personal health information of family members? If such consent is granted, what are the rights of those family members?

Among those risks which the Committee and the Government must grapple with is the risk to privacy. As we noted in our initial submission, there have been experiences in places such as Iceland where personal health information derived from genetic testing has been removed from the jurisdiction and from the regulatory control of that government. When we contemplate large scale private sector research involving the collection of genetic information about citizens of this Province, it is crucially important that we try to anticipate any circumstances in which that personal health information might escape provincial oversight, through such events as a sale of assets, a sale of the company, a bankruptcy, a move by the company to another jurisdiction, etc. It is also important that we do not craft a provision tailored to Sequence Bio that wouldn't address a company based elsewhere in Canada or the world wishing to pursue similar projects in this Province.

In our initial submission, the OIPC attempted to explain this concern and propose one possible legislative approach to mitigate it. That concern was also highlighted by other stakeholders, who proposed similar measures. In its submission, Sequence Bio recognizes that some degree of regulation and oversight of its activities will in fact facilitate progress towards their goals and objectives. Sequence Bio proposes a means of addressing the issue by recommending that some of Sequence Bio's activities be subject to *PHLA*. The approaches suggested by the different stakeholders are not entirely dissimilar.

We do not wish to say that the recommendation put forward by the OIPC is the best or sole solution to all of these challenges, however the important thing to emphasize at this point is that there seems to be some degree of consensus on the essential issue to be addressed. The ultimate solution, if there is one, must be a legislative amendment which ensures that the personal health information of citizens of this Province will not be misused or removed from the regulatory oversight of this jurisdiction.

Newfoundland and Labrador Medical Association (NLMA)

The submission of the NLMA covered several topics. Three recommendations were made regarding “circle of care”. The first was that the definition should be included in section 2 of *PHIA*. In our view, “circle of care” is already defined in section 24, however if it was determined that there is value in including it within the definition section of *PHIA*, a provision similar to 2(1)(f) would suffice, in which the definition of the term would be “as described in section 24.”

The second recommendation, that family physicians automatically be considered to be in the circle of care unless a patient expresses otherwise is probably redundant. It is agreed that on face value, the family physician is generally responsible for coordinating care by other professionals and providers, and would in most cases fall within the circle of care anyway. We appreciate that care can be disjointed and that silos may exist between disciplines and programs, but this is a matter of improving standards of professional practice. It is not clear from the information provided that a misunderstanding or misapplication of the term “circle of care” is the cause of this situation, nor would the proposed amendment necessarily be the solution even assuming there is a problem.

The NLMA’s third recommendation on circle of care is “a consistent interpretation and use of the circle of care and communication on this definition to all custodians and their employees.” As noted, section 24 contains a clear definition of the term at issue. Resources are available on the Department of Health and Community Services web site which discuss the concept in more detail. If there has been inconsistent interpretation of the term, this Office is willing to discuss the matter and help sort out differing approaches. Ultimately, however, section 13 of *PHIA* requires each custodian to develop policies and procedures regarding collection, use and disclosure of personal health information. The OIPC is available as a resource to review draft policies and procedures to help ensure that they remain consistent with the language in *PHIA*.

The NLMA also discussed the term “agent” in its submission, indicating that the term is not well understood or consistently applied. We agree. The Canadian Nurses Protective Society, according to how it uses the term in its submission, appears to be operating with a very expansive view of the term which seems to include all nurses. There may be an opportunity to better define this term in *PHIA*, or at least to provide examples of its correct use. We are willing to work with the Department, RHAs and other custodians to further refine it either in legislation or in policy.

We support the NLMA recommendation that all custodians be involved in further discussion about the use of consent directives in information systems. It is clear that there are many shortcomings in how this process currently operates, leaving patients with less control over their personal health information than is intended by *PHIA*.

Finally, the NLMA provided some commentary about reforming the health care system. Among the comments was a statement that “physicians are concerned that the interpretation and implementation of section 15 must not place information protections that make it impossible to modernize the health system.” The NLMA then discusses various advances in the use of technology that may improve the health care system, and the concern is expressed that section 15, which is the security provision of *PHLA*, may hinder such progress. It should be noted that section 15 requires “steps that are reasonable in the circumstances,” and it is this standard that the OIPC will apply. That being said, we believe that the adoption of new technologies in the collection, use and disclosure of personal health information requires appropriate scrutiny. This is typically accomplished through a Privacy Impact Assessment (PIA), which has been recognized across Canada and around the world as a reasonable step to take prior to implementing such a new program or service. The OIPC stands ready to consult at any stage in the PIA process and to assist custodians in moving new programs and services towards implementation. The OIPC discussed and provided recommendations regarding PIAs in its initial submission.

Memorial University

Although Memorial has productively engaged with this Office on many issues over the years, and in fact has played a positive role in the promotion of access to information and protection of privacy, there have been occasions where we have been critical of Memorial’s position on certain matters, and there have also been areas of profound disagreement. The following issue is fairly placed in the latter category.

A number of points were raised by Memorial in its submission which require a response. Memorial argues that the four schools/faculties that are currently designated as custodians subject to *PHLA* should no longer be custodians and therefore no longer subject to the *Act*. It is already clear from the comments in our initial submission that we take the opposing view. Our initial submission briefly summarized our position on this issue, in which we took the view that the *Health Research Ethics Authority Act (HREA)* and *PHLA* are intended to operate *interdependently*, and we note that *HREA* lacks a complaint investigation mechanism available to the general public to protect the privacy rights of individuals whose information may be used in research approved by a Research Ethics Board. There are, however, additional points that can be made in favour of retaining these schools/faculties as custodians subject to *PHLA*.

Memorial has in the past opposed our jurisdiction to carry out our privacy and access to information oversight role in several contexts (see our Report P-2011-002 for example). [Report P-2011-002](#) investigated a privacy breach involving researchers employed by Memorial University. Among other things, Memorial refused to provide the Commissioner with documentation detailing the information which researchers were approved to collect by the Human Investigations Committee. If a new complaint of that nature arrived today, under *PHLA*, that information would be essential in order to determine compliance with section 44 of *PHLA*, ie, whether a disclosure which has occurred accords with the approval granted by a research ethics board. It should be noted that the events covered in the Report occurred prior to the proclamation of either *HREA* or *PHLA*, and that the version of *ATIPPA* referenced in the Report has also been superseded by the *ATIPPA, 2015*, so much of the discussion hinging on legislative interpretation is moot. However, paragraphs 85 through 88 remain relevant considerations in assessing the relationship of faculty members to Memorial University in the conduct of their research.

An aspect of the jurisdictional issue expressed by Memorial from time to time over the years is the assertion that many of the activities of its academic employees are not within the scope of their employment duties at Memorial and therefore many of the records associated with those activities are not within the control or custody of Memorial. For example, Memorial has argued that the research data researchers obtain in the course of discharging their contractual obligation to conduct research as per the MUNFA agreement is in fact in the individual custody and control of each researcher, and not in the control or custody of Memorial. This is despite the fact that research funding applications are made by these researchers under the auspices of Memorial University, funding for the research is processed and administered through Memorial's Office of Research, faculty members are required to engage in research under their collective agreement, and researchers seeking approval through a Research Ethics Board present themselves as having all of the institutional support of Memorial behind them. This often includes elements such as data storage and security, and policies and procedures to protect the data from unauthorized access, use, disclosure, loss, theft, and to ensure its secure destruction under terms required by the REB.

It is well-known that graduate and post-graduate students as well as faculty move to other universities throughout the course of their career. It is unclear whether Memorial expects that such research data could be taken with these researchers personally to their new appointments. Alternately, it is unclear whether Memorial intends to undertake, either through an agreement with all researchers, or by default, to maintain the security of such data after the departure of researchers. If these schools/faculties remain as custodians, some form of accountability will be maintained for such research data. If not, accountability becomes very elusive, and risks to privacy become much more significant.

On November 27, 2014 a government news release announced the TPM Initiative. This is a significant new venture which will no doubt bring many benefits to the public. Having *PHLA* continue to apply to the current custodians at Memorial has not, to our knowledge, interfered with the laudable goals outlined in the news release. Rather, the interconnected statutory regime of *PHLA* and *HREA* ensures that there are standards in place which establish clear lines of accountability. The following links provide information about this initiative:

<http://today.mun.ca/news.php?id=9279>

<http://www.med.mun.ca/Medicine/Faculty/Staff/Faculty-Handbook/Research/Research-Support/Patient-Oriented-Research.aspx>

It is clear through the example of such initiatives as TPMI that the Faculty of Medicine is currently a custodian of a large amount of personal information. It is important to note that even if personal information has been de-identified, if the data can be re-identified then it still requires protection. Furthermore, there are other risks associated with small sample sizes and our rural population which means that personal information that has been nominally de-identified may in fact be readily re-identifiable.

Another point which is not fundamentally a privacy issue, but more of a practical concern, is perhaps the unintended consequence of de-listing these custodians at Memorial. Amending *PHLA* as proposed by Memorial may in fact affect the willingness of custodians such as Eastern Health, NLCHI, or any other custodian of personal health information to disclose data to researchers.

In its submission to *PHLA* Review, NLCHI has clearly advised that it has concerns about this proposed amendment. As a custodian of personal health information, NLCHI must decide when and under what conditions to disclose personal health information at the request of a researcher. Approval by the REB is simply a pre-requisite – NLCHI must also satisfy itself that the disclosure is appropriate and any risks can be mitigated. After all, the REB process, while having elements of data security and ethics, is not explicitly a privacy review.

NLCHI therefore operates on a trust model, and it is our understanding that this is not an uncommon approach. NLCHI advises in its submission that this is a two-tier model. Currently, researchers from Memorial applying for data from NLCHI are accorded a higher degree of trust than independent researchers because the schools/faculties with which they are affiliated are custodians subject to *PHLA*. NLCHI advises that the change in status proposed by Memorial “would impact the disclosure of data to researchers affiliated with that organization.”

Eastern Health also commented in its submission on the application of *PHLA* to personal health information used in research. Contrary to Memorial’s view, Eastern Health has recommended expanding the coverage of *PHLA* to include all post-secondary institutions whose employees are conducting research involving personal health information, as well as expansion of *PHLA* coverage at Memorial University beyond the four schools/faculties currently listed. It should be noted that Eastern Health, like NLCHI, is also a custodian which frequently receives requests from researchers at Memorial for personal health information. Clearly, Eastern Health is more comfortable disclosing personal health information to a researcher affiliated with an institution that is designated as a custodian under *PHLA* and would prefer to operate under that model in its relationship with the research community.

In its submission, Memorial repeatedly emphasizes that the REB process is in place, and it is proposed that any requirements on researchers flowing from that process are sufficient. The submission of the HREB takes the opposite view. HREB makes the point that the REB process is not intended to serve as a *PHLA* lens on the proposed research process. HREB emphasizes that custodians should conduct their own reviews of research requests in addition to the REB process. Based on the submissions provided, Eastern Health and NLCHI take the approach recommended by HREB, and one of the factors considered by those custodians which supports the decision to disclose is whether the receiving party is also a custodian or employee of a custodian. This is simply part of the risk analysis that it is incumbent upon Eastern Health and NLCHI to apply when receiving requests for personal health information from researchers, and it is supported by HREB. In fact, HREB would like to see language in section 44 of *PHLA* strengthened to emphasize this responsibility on the part of custodians who receive requests for information from researchers. Simply put, the status of custodian is a significant factor which plays into the decision to disclose data to researchers, because it provides a level of assurance that the information will remain secure, and that there is accountability for maintaining that security.

The submissions of NLCHI, Eastern Health and *HREA*, in our view, clearly demonstrate that the statutory regime that exists currently is not a barrier to research, but instead is an asset which supports research by providing the assurance of clear legislated accountability. We would therefore recommend that further consideration be given to the recommendations of Eastern Health and *HREA* that section 44 be clarified and that coverage of *PHLA* be broadened to include other educational institutions which are carrying out research involving personal health information.

Memorial's submission asserts that, among other reasons, the schools/faculties should not be included as custodians because "the delivery of health care services does not fall within Memorial's mandate." This statement is not a relevant consideration, when one refers to section 3 of *PHLA*, where six separate purposes for the *Act* are outlined, including "to establish rules for the collection, use and disclosure of personal health information that protect the confidentiality of that information and the privacy of individuals with respect to that information." Nowhere in section 3 or anywhere else in *PHLA* is it indicated that the *Act* is only intended to cover personal health information which resides with a body that is directly engaged in the delivery of health care services.

On page 3 Memorial states *PHLA* "potentially creates various impediments to research and the development of intellectual property and undermines existing practices in academia around research data custody and control." These various potential impediments are not listed in the submission. Furthermore, even if it is accepted at face value that *PHLA* has any impact on "existing practices in academia" it is not at all clear that such impacts are substantial or even negative. In fact, as noted above, the argument put forward by NLCHI and Eastern Health is that being subject to *PHLA* has assisted researchers in accessing data by providing a level of trust and assurance associated with the application of *PHLA* to the schools/faculties which would not be possible if researchers' data requests were to be evaluated independent of such an affiliation.

Memorial quotes at length the Tri-Council Policy Statement regarding the importance of academic freedom. It is not clear how *PHLA* undermines this. This Statement says that researchers have an obligation to maintain ethical standards that protect and respect the participants. Certainly if Memorial University became aware of an unethical practice on the part of one of its researchers, it would not sit idly by and do nothing. By being subject to *PHLA*, the schools/faculties simply facilitate and ensure that a law is followed that protects and respects research participants. If there is an example of how the application of *PHLA* has negatively impacted the conduct of research by researchers at Memorial in the nearly 6 years it has been in force, it is presumed that such information would have been laid before the *PHLA* Review Committee.

On page 4 of its submission Memorial refers to the importance of protecting the trust relationship between a researcher and his or her research subject. Such a relationship would more than likely involve direct collection with consent. Of course, it should be noted that section 44 of *PHLA* facilitates disclosure of personal health information to a researcher *without* consent, which means that there is no trust relationship with the research subject, only between the disclosing custodian and the receiving party. Our argument is simply that the receiving party must be subject to *PHLA* in order to better ensure the protection of the research subject, who is unaware that this disclosure has occurred.

The concern is also expressed by Memorial that research data may "potentially" create an obstacle to academic freedom because under *PHLA* the Commissioner could "potentially" access the information during an investigation. Section 71 of *PHLA* ensures that this power is used sparingly by the Commissioner. It should be noted that, although issues have arisen under *ATIPPA* on a couple of occasions, there have been no demands by the OIPC for research information from Memorial University under *PHLA* to date. Furthermore, the purpose of any such investigation, should one occur in the future, is to protect the interests of the research subjects. This might occur, for example, as a result of a complaint from a person who has been a research subject. Even if it were to occur, the investigation would be limited to issues which arise under *PHLA*, and there would be no hindrance of academic freedom. In this sense, having *PHLA* applicable, even if it has so far not been

used in an investigation in a research context, is in fact an asset allowing researchers to demonstrate that potential research participants and disclosing custodians can have confidence in the research endeavor, because there is oversight and recourse in the case of a complaint.

Further along on page 4 of its submission, Memorial says once again that “subjecting research data to *PHIA* also **potentially** creates impediments to research generally by imposing obligations on researchers at Memorial that are not imposed on researchers in private industry ... or on other institutions...”[emphasis mine]. Again, we have no evidence of these alleged impediments. It is acknowledged that proper administration of *PHIA* by the named custodians at Memorial should entail some administrative responsibility, however this is actually in service of the researchers because it allows the researchers to rely on the policies and procedures and security arrangements of a large institution, which carries a great deal of value at an REB or for a custodian considering whether or not to disclose personal health information.

I note the concern expressed that Memorial is not being treated fairly because other parties may not have to comply with *PHIA*. Interestingly, we see in the submission of Sequence Bio, a private sector entity, that they wish to come under the *PHIA* umbrella because of the value it provides. Furthermore, we see Eastern Health suggesting that *PHIA* be expanded to cover other entities engaged in research. What Memorial is attempting to evade is actually considered to be an asset elsewhere. Further to Memorial’s comment about the advantages of private sector researchers, a private sector researcher would likely be subject to *PIPEDA*, which would likely subject such a company to the access and correction provisions of that statute.

Again, further along on page 4 of its submission, Memorial talks about “potentially” slowing research, and it expresses concern that “applying *PHIA* to research data could also threaten the commercial viability and value of intellectual property” generated from research. Unfortunately, we are not provided with any evidence that this is the case. However, assuming for the moment that there is evidence or that this is a real cause for concern, it would be a much more productive exercise to look at the specific provisions within *PHIA*, whether it is access, correction, or mandatory disclosure, which are the root of the concern, and see if there is an amendment necessary to deal with a real problem.

Memorial also notes that the *Personal Health Information Protection Act (PHIPA)* in Ontario does not name universities or academic units as custodians. It should be noted that *PHIPA* provides for a completely different regime for the protection of privacy in the course of research, and furthermore Ontario does not have an equivalent to *HREA*, so the comparison is not “apples to apples”.

In a legislative review process, it is important to not only look back at how the law has functioned, but also to look ahead to the demands and expectations of the coming years. The Organization for Economic Cooperation and Development (OECD) in January 2017 published a [recommendation](http://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf) containing 12 principles on health data governance:

<http://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf>

This recommendation is intended to apply to all 35 member countries, including Canada, and it is intended to advance and facilitate access to data for research purposes. The process to develop this recommendation was advised by an Expert Group, including well-known Canadians, former Privacy

Commissioner of Canada Jennifer Stoddart and leading health research ethicist, Professor Bartha Knoppers. Among the 12 principles are the following:

10. Establishment of appropriate training and skills development in privacy and security measures for those processing personal health data, that are in line with prevailing standards and data processing techniques.

11. Implementation of controls and safeguards. These should:

- i. Provide clear and robust lines of accountability for personal health data processing, accompanied by appropriate mechanisms for audit.*
- ii. Establish requirements that personal health data can only be processed by, or be the responsibility of, organisations with appropriate data privacy and security training for all staff members, commensurate with their roles and responsibilities in relation to processing personal health data and consistent with any applicable professional codes of conduct.*
- iii. Encourage organisations processing personal health data to designate an employee or employees to coordinate and be accountable for the organisation's information security programme, including informing the organisation and its employees of their legal obligations to protect privacy and data security.*
- iv. Include formal risk management processes, updated periodically that assess and treat risks, including unwanted data erasure, re-identification, breaches or other misuses, in particular when establishing new programmes or introducing novel practices.*
- v. Include technological, physical and organisational measures designed to protect privacy and security while maintaining, as far as practicable, the utility of personal health data for health-related public interest purposes. Such measures should include:*
 - a. Mechanisms that limit the identification of individuals, including through the de-identification of their personal health data, and take into account the proposed use of the data, while also allowing re-identification where approved. Re-identification may be approved to conduct future data analysis for health system management, research, statistics, or for other health related public interest purposes; or to inform an individual of a specific condition or research outcome, where appropriate.*
 - b. Agreements, when sharing personal health data with third parties for processing that help to maximise the benefits and manage the risks while maintaining the utility of personal health data. Such agreements should specify arrangements for the secure transfer of data and include appropriate means to effectively sanction non-compliance.*
 - c. Where practicable and appropriate, considering alternatives to data transfer to third parties, such as secure data access centres and remote data access facilities.*
 - d. Robust identity verification and authentication of individuals accessing personal health data.*

12. Require organisations processing personal health data to demonstrate that they meet national expectations for health data governance. This may include establishment of certification or accreditation of organisations processing personal health data, in so far as these certifications or accreditations help to implement standards for the processing of personal health data or demonstrate capacity to meet recognised governance standards.

It is apparent in reviewing this document that it would be impractical to place such burdens on individual researchers. The clear intention is that health data governance accountability is best placed at an institutional level in an organization that has the capacity to deliver on these requirements (such as, in this jurisdiction, Memorial University or designated schools or faculties therein). Any organization that is prepared to comply with the mandate outlined above should have no trouble complying with *PHLA*. *PHLA* compliance would then provide the assurance to the public and to custodians who are asked to disclose personal health information that appropriate oversight is in place. Given that this standard has been “welcomed by Health Ministers” representing OECD membership, it appears to represent a consensus on the way forward for health data governance in the 21st century.

If *PHLA* were to be out of the picture for personal health information at Memorial, there would be no legislated requirement for information security policies and procedures; no complaint mechanism for the public if someone believes their information has been collected, used or disclosed improperly in the course of research activities; and no real oversight of the privacy rights of citizens whose information is used in research activities.

There are no provisions for a complaint from the general public through *HREA* and no investigative processes available to the public through *HREA*. *PHLA* is currently the only recourse for members of the public who believe their information has been misused in a research context by one of these custodians. It is worth noting that there have been rare and isolated cases in other jurisdictions where custodians or their employees have illicitly sold personal health information for profit, or engaged in other gross misconduct. Again, the regime in place under *PHLA* would allow for appropriate accountability actions to take place in such an extreme circumstance, including the prosecution of such acts as an offence under *PHLA*.

Memorial has asserted throughout its submission that *PHLA* is somehow a barrier to research. With respect, Memorial has offered no evidence to support that claim. *PHLA* is no more an impediment to academic freedom than *HREA*. Contrary to the assertion by Memorial that the protection of privacy through *PHLA* is an impediment, other participants in this Review, on whom researchers depend for access to data, have clearly stated that the privacy standards associated with *PHLA* are in fact making access to data smoother and easier for Memorial researchers, and that removing the schools/faculties as custodians is likely to create a barrier to data access which does not currently exist.

Canadian Nurses Protective Society (CNPS)

CNPS raises a number of issues in its submission. With all due respect, the OIPC disagrees with most of the recommendations and suggestions proposed by CNPS. The following comments will address the most noteworthy of these.

The first significant issue is related to the observation that the policies and procedures of custodians required by *PHLA* under section 13 are intended to be legal obligations in accordance with 14(2)(b) of *PHLA*. CNPS objects to this as being burdensome for custodians “who are required to anticipate any and every situation in which every employee may have to make decisions with respect to the collection, use and disclosure of PHI.” On the one hand, it is our experience that smaller custodians

seem to have had great difficulty coming to terms with the requirement to have policies and procedures, and this is an issue which the *PHLA* Review Committee may wish to address. On the other hand, the description that such policies and procedures must “anticipate any and every situation” vastly overstates the requirement. An interesting point made by CNPS however is its observation at the top of page 4 of its submission that there is no process to review or ensure that the content or application of policies and procedures adopted by a custodian is in accordance with *PHLA* (or other statutes). As we have stated elsewhere, the OIPC stands ready to review and comment on any draft policies and procedures prepared by a custodian with the goal of helping to ensure that they are compliant with *PHLA*, however in practice this has rarely occurred. Furthermore, it is expected that policy and procedure documents of the RHAs would be publicly available, and if CNPS wishes to review same and provide comments to the RHAs, that is also an option.

CNPS also states that nurses as health care professionals have certain legal and professional obligations. CNPS proposes that *PHLA* expressly authorize regulated health care professionals to collect, use, and disclose personal health information to meet their professional obligations. CNPS says on page 5 of its submission that *PHLA* does not contain “express authorization” for certain disclosures, however *PHLA*, like other health information statutes in Canada, does not contain a provision for every circumstance. It is our view that *PHLA* as it stands is designed to allow for the appropriate collection, use and disclosure of personal health information by health professionals, whether they are employees of a custodian, agents of a custodian, or acting as a custodian in their own right.

CNPS expresses concern that certain disclosures which registered health professionals are obligated to make might be contrary to *PHLA*. That does not reflect our reading of *PHLA*, although the process for making such a disclosure should be addressed through a custodian’s policies and procedures. It would be useful to know whether there have been any cases in this Province where a nurse believed that *PHLA* interfered with a professional obligation to report (disclose personal health information) under *the Children and Youth Care and Protection Act*, the *Highway Traffic Act*, or the *Adult Protection Act* listed as examples by the CNPS. The vast majority of nurses in this Province are employed by one of the four Regional Health Authorities (RHAs). If this issue is a concern for CNPS, it is suggested that CNPS may wish to review and provide comment to the RHAs about any perceived gaps in the policies and procedures of the RHAs.

It is noted that CNPS, throughout its submission (the middle paragraph on page 7 for example) refers to nurses as “agents”. Other submissions to the *PHLA* Review Committee have expressed some uncertainty regarding the definition of agent. In our view, nurses employed by Regional Health Authorities are not agents, but are simply employees. While there is no definition of “employee” provided in *PHLA*, provisions like 13(2)(b) and 14(2) demonstrate that employees and agents are intended to be separate categories because they are listed separately. The principles of statutory interpretation tell us that the decision to use different terms in a statutory provision means that they are intended to have different meanings. There may be other nurses who are in fact agents who occupy other roles, but this would be very much the minority.

We disagree with the suggestion at the top of page 8 that the requirement to comply with a custodian’s policies and procedures is “superfluous”. Removing the requirement for policies and procedures would undermine the entire structure of *PHLA*, which we do not see as productive. Later, on page 8, CNPS says that “*PHLA* does not stipulate whether the employer’s authorization to

collect, use or disclose PHI can be implicit or if it must be an express authorization.” We are of the view that sections 24 and 25 adequately address this issue, and that RHAs are covered by section 24(2). CNPS says that “... it has been our experience that some employers have concluded that employees inappropriately accessed PHI when this was done without express authorization.” If there are grievance awards, court decisions or other documents available which might demonstrate this, we would be interested in seeing them. In our interactions with RHAs, we have not encountered such a circumstance. We have, however, seen this conclusion drawn when the patient was not in the circle of care of the nurse in question.

On page 9 CNPS discusses issues relating to procedural fairness, and notes that *PHLA* does not contain any specific provisions which ensure that procedural fairness must be followed by an employer when attempting to determine whether personal health information has been inappropriately accessed. It is our understanding that such provisions are not common in personal health information statutes, but would be expected in human resources processes such as grievances and investigations by employers. This is an area that is well understood within the field of labour law, and it is not something we anticipate would find a home in *PHLA*. Any disciplinary finding or measure imposed by an employer based on its policies or procedures, whether or not they are *PHLA* policies or procedures, is a matter between the employee and employer, unless the matter comes before the Commissioner and it is determined that an offence under section 88 of *PHLA* may have been committed. In such a case, the assessment of any issues relating to procedural fairness is a matter for the courts.

On page 14 CNPS asserts that the circle of care provision is inadequate. In our view, the language in section 24 is sufficiently broad to capture all of those persons and activities appropriately considered to be in the circle of care. CNPS says that “... the concept of ‘circle of care’, as it applies to agents of custodians nonetheless is often given a very restrictive interpretation.” CNPS does not say who has provided this restrictive interpretation and what effects it may have had. Through our regular discussions with RHAs we have not been advised of these types of difficulties and we do not support the recommendation of CNPS.

Appendix B-3



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

March 23, 2017

Dr. David Morgan
PHLA Review Committee
P.O. Box 8700
1st Floor, West Block, Conf. Bldg.
St. John's, NL A1B 4J6

Dear Dr. Morgan:

I note that the other Third Round Submissions in the *PHLA* Review process were all from Regional Health Authorities (RHAs), and furthermore a large proportion of their comments were in relation to recommendations which were made by the OIPC in its initial submission. Upon review and consideration of the comments offered by the RHAs, some clarification of the OIPC's position on these topics may be of assistance to the *PHLA* Review Committee.

One of the topics which attracted commentary from the RHAs was the recommendation by the OIPC that certain large custodians, including the RHAs, complete privacy impact assessments (under conditions explained in our submission) and provide those to the OIPC for review and comment. In our initial submission, we failed to note that there will be times when a preliminary privacy impact assessment (PPIA) would be sufficient. Section 2(w) of *ATIPPA, 2015* defines a PIA as "an assessment" but it does not specify a particular form or depth of analysis. Our conception of this process would be that this assessment can take the form of either a PPIA or a PIA as the circumstances warrant. As noted by the RHAs, PIAs are already a standard operational procedure, whether these be produced in cooperation with other RHAs or produced individually by one RHA. The word that is used by the RHAs in some of their responses is a "formal" PIA. The interest of the OIPC is in being able to provide input on the assessment which has been conducted by an RHA of the privacy considerations of an undertaking, whether that be a PPIA or a PIA. Our interest is in the content of the assessment, rather than the length or format.

Another point which we failed to address was brought to light in the concerns expressed about how our review process might result in slowing down the implementation of a new program or process. Of course, it is inherent in any PIA process that privacy risks may be identified and mitigation measures implemented to address those risks. That process may result in a delay whether or not the OIPC is involved. It is possible that through review by the OIPC that questions which had not been previously considered about a new program or process may be raised. The intention of raising such questions would be to ensure that the program or process is compliant with PHIA, and we do not expect that any of the RHAs would want to proceed with a program or process with unmitigated, unacceptable risks attached. In terms of the time required by the OIPC to review a PIA or PPIA and provide feedback, we can commit, and we would support this being incorporated into legislation, that our review, including any written feedback or commentary, will be provided within 30 days, with an extension of 30 days allowable only in extraordinary circumstances.

Another issue that was raised by the RHAs was in relation to our recommendation that the response time for an access request be decreased from 60 days to 30 days. Given the challenges currently faced by the RHAs in light of the added responsibility represented by our recommendation of PIA/PPIA review by the OIPC, we withdraw that recommendation.

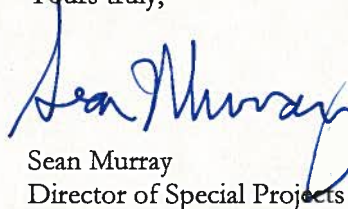
Central Health refers in its submission to "the current provincial fee schedule". It should be noted that there is no provincial fee schedule that applies to all custodians. There is a fee schedule that has been agreed upon by the RHAs, and in our Supplementary Submission on page 3 we support it. However, there is currently no guidance to all custodians as to what is considered to be a "reasonable" fee in accordance with section 57 of *PHLA*. There is some commentary by a couple of RHAs to the effect that there should be some element of cost recovery involved. In our Supplementary Submission we reference our Report AH-2012-001, which considers differing approaches to fees based on differing legislative language used in various jurisdictions. We stand by the principle that the most important factor is that the information being requested is in fact the personal health information of the applicant and assessing the reasonableness of the fee is an exercise that is primarily intended to be oriented towards the right of the applicant to obtain access.

Another comment offered in the recent submission of Central Health on pages 2 and 3 is in relation to a suggested revision to section 14(2)(b) where it is proposed that "in accordance with accepted professional practice" be added. This could be problematic. For one thing, the rationale assumes that accepted professional practice is potentially in conflict with *PHLA*, whereas our view is that *PHLA* was designed to be largely complementary to professional practice standards. The difficulty is that those standards are not spelled out in *PHLA*, but are included in other statutes and/or guidelines. Including such a provision may have the effect of undermining *PHLA* if there are differing views as to what may constitute accepted professional practice. Furthermore, in the case of serious breaches leading to prosecution, it may significantly hinder a prosecution if witnesses are brought in to testify that "professional practice" justifies the breach and/or are unable to agree on what it means in a given case. In the first prosecution undertaken in this Province under *PHLA*, the accused, who was a nurse, offered the defense that her inappropriate access was actually within the scope of accepted professional practice. She was found guilty of the offence, but if such a provision was added to *PHLA*, the line will become so blurred as to potentially preclude *PHLA* prosecutions involving registered health professionals.

Central Health also addressed our recommendation that all privacy breaches reaching the threshold requiring notification to affected individuals also be reported to the Commissioner. The point that perhaps could have been more fully addressed in our original recommendation was that the rationale for this is related to the ability of the OIPC to monitor compliance with *PHLA*. The value of breach reporting is represented not only in the details of a particular breach, but in being able to monitor and evaluate trends, and allowing this to inform training and education with the goal of preventing or avoiding similar breaches. This was also addressed by the *ATIPPA* Review Committee in the section entitled "Conclusion" on page 177: http://www.oipc.nl.ca/pdfs/ATIPPA_Report_Vol2.pdf. The Review Committee recommended that all breaches be reported to the Commissioner, and this recommendation was accepted and is part of the law. With regard to *PHLA*, our recommendation was that the OIPC only be informed of those breaches which meet the threshold of requiring notification to affected individuals.

I trust this additional input will be of some value. As always, if you have any further questions please do not hesitate to contact me.

Yours truly,



Sean Murray
Director of Special Projects

Appendix C



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

May 4, 2023



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

May 4, 2023

VIA EMAIL

Mr. John McGrath
Associate Deputy Minister
Department of Health and Community Services
JohnMcGrath@gov.nl.ca

Dear Mr. McGrath,

Subject: OIPC PHIA Review Submission

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*.

Please do not hesitate to contact our office 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 aspects of *PHIA* that we have not already addressed.

Yours truly,

Michael Harvey
Information and Privacy Commissioner

Copied to:

Donna Roche, Director
Data Governance and Privacy
Dept. of Health and Community Services
DonnaRoche@gov.nl.ca

Carole Piovesan, Principal/Co-Founder
INQ Consulting
cpiovesan@inq.consulting

Angela Power, Senior Director, Ethicist
INQ Consulting
apower@inq.consulting

Justin Caines, Legislative Consultant
Dept. of Health and Community Services
JustinCaines@gov.nl.ca

Samara Starkman
Managing Principal/Co-Founder
INQ Consulting
sstarkman@inq.consulting

David Goodis, Advisor
INQ Consulting
dgoodis@inq.consulting

Introduction

The Office of the Information and Privacy Commissioner appreciates the opportunity to participate in this Statutory Review of the *Personal Health Information Act*. In the unusual circumstances of this statutory review, in which the report of a previous statutory review addresses many of the outstanding issues with *PHIA*, and no statutory amendments resulted from that review, our written submission will be relatively brief.

Three substantial areas we addressed in our 2017 submission were (a) that attention should be given to how custodians are defined to avoid confusion about who are the custodians where multiple parties might be considered a custodian, leading to accountability issues; (b) that *PHIA* currently provides OIPC with Ombud-style oversight rather than the hybrid role adopted by *ATIPPA, 2015* and this hybrid role should be incorporated within *PHIA*; and (c) that the roles and responsibilities of researchers vis-à-vis their institution (Memorial, principally) needs greater clarity. To a large extent, we are of the view that the 2017 statutory review submission remains relevant and the vast majority of its recommendations would, if implemented, improve the statute. We therefore suggest that those recommendations be put forward to the Minister again, proposing that *PHIA* be amended accordingly, with certain caveats that will be outlined below.

Further, in addition to these few areas in which we diverge from the 2017 *PHIA* recommendations, we are of the view that certain additional matters have risen in importance since that time, which warrant consideration in the current review. The first of these is Artificial Intelligence (AI).

Artificial Intelligence

The [Final Report of the 2020 ATIPPA Statutory Review Committee](#), issued in June 2021, contains a discussion (starting at page 372) and recommendations regarding the inclusion of provisions related to AI, which largely resulted from and reflected recommendations we made beginning at page 35 of our [submission](#) to that review process. In this submission we will be making a similar recommendation. As we have discussed in our consultations, AI development and integration into everyday life is moving fast, and it involves vast amounts of data, often personal information, to accomplish tasks at a scale and impact that are breathtaking. In many cases, depending on the particular AI tools employed, we may not fully understand how these tasks are accomplished, whether the result is good or accurate or beneficial, and whether the models employed can in some cases even fit within the long-recognized paradigm of the ten privacy principles. This is a lot to consider, given the short time frame within which AI seems to have emerged into the public consciousness, but the exponentially increasing investment in AI that is presently occurring makes it almost certain that it is only a matter of time before we learn of its presence and use within the provincial health care system. In fact it may already be there given the plethora of different prognostic and diagnostic tools that are emerging on a rapid basis.

Considerations regarding AI are arguably even more important in the *PHIA* context than in *ATIPPA*, at least at this stage of the development of AI. The health sector is a very data rich and highly innovative sector with involvement of national and multi-national vendors, and therefore it might reasonably be expected that the health sector is one of the sectors where AI is most likely to penetrate at an earlier stage. Moreover, if AI is being used in the health sector, then the implication is that decisions using AI are likely to affect the provision of clinical care directly or indirectly, so the stakes are very high.

One concern we have heard regarding Chair Orsborn's recommendation relates to the proposed definition of "automated decision system", is that it may be overbroad, capturing simple automated decision-making processes that don't require additional privacy protections or oversight. We would be amenable to a different definition that captures automated processes where real privacy risks and ethical considerations are more likely to be present.

For example, one option would be to adopt or adapt the definition from Bill C-27 which is before Parliament at the time of writing:

artificial intelligence system means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.

Alternatively, Quebec's Bill 64 has added the following provision to its privacy law:

65.2. A public body that uses personal information to render a decision based exclusively on an automated processing of such information must inform the person concerned accordingly not later than at the time it informs the person of the decision. It must also inform the person concerned, at the latter's request,

(1) of the personal information used to render the decision;

(2) of the reasons and the principal factors and parameters that led to the decision; and

(3) of the right of the person concerned to have the personal information used to render the decision corrected.

While the federal law focuses on automated systems that are at least "partly" autonomous, no such distinction is made in Quebec's law. Interestingly, the federal law ensures that regulation only kicks in at a relatively high level. As noted, it only applies to autonomous or partly autonomous systems, so it does not regulate even the most complex automated systems that could use personal information to make decisions about people, potentially remaining opaque to consumers while making significant decisions that may affect their lives in myriad ways, if such a system is not at least partly autonomous. Furthermore, a private sector AI system must have a "high impact" outcome in order to fall within the scope of the Act. Given that the federal government has a clearly stated goal of fostering growth of the AI

industry in Canada, it makes sense that it would want to ensure a minimal regulatory footprint, while ensuring that provisions are in place to regulate high impact systems.

Quebec's law addresses AI in both the public and private sectors, but the specific section quoted above is meant to apply entirely to public sector entities. For anyone who has compared private sector versus public sector privacy statutes in Canada, the distinction between Quebec's law and the federal law is understandable. Private sector privacy laws have traditionally been built on consent, meaning that the consumer voluntarily provides their personal information to a particular business for the purpose of obtaining goods and services. While concepts of consent are evolving to reflect that there are circumstances in which it is simply not reasonable to collect, use or disclose certain personal information of consumers in certain circumstances, ultimately the concept of consent is still central.

With public sector entities, however, it is often the case that laws require or permit public bodies to collect, use or disclose personal information for many different purposes. If you want a hunting permit, for example, you must provide the information that is required by statute for that purpose. There is no competing government in your jurisdiction that you can go to and provide less personal information to get a hunting permit. While consent is not absent from these statutes, it very much takes a back seat to a public body's processes in carrying out its legally authorized mandate. Essentially, when it comes to public bodies, including public sector custodians of personal health information, we don't really have much choice about what information to provide if we are to obtain the services we are entitled to as citizens. On that basis, it seems more appropriate to adopt a broader view of AI regulation such as that found in Quebec's Bill 64 for our health care system, and for *PHIA*. Even though *PHIA* covers both public and private sector custodians, a greater portion of the health care system is a public system, and therefore should reflect the characteristics that are common to that system.

One important aspect of our recommendations that Chair Orsborn recognized was that the broader positive and negative public impacts of artificial intelligence are not limited to privacy risks, yet realistically, at least in smaller jurisdictions such as this one, there is no other oversight body equipped to consider those broader ethical impacts on society at large:

But since the OIPC is the only privacy oversight body in the public sector, and given that the creation of an additional oversight commissioner is unlikely, it is appropriate to now suggest amendments to ATIPPA, 2015 that authorize a level of oversight for proposed artificial intelligence applications. Some may argue that allowing the OIPC to comment on the "ethical implications" of a proposed automated decision system – that is, commenting on issues not directly related to access and privacy – takes the Act outside its present intended scope. There is merit to that argument, but, at least until there is specific legislation governing all aspects of development and application of automated decision systems, the most appropriate – indeed perhaps the only – means of ensuring consideration of these issues lies within ATIPPA, 2015.

Our concern regarding AI oversight is that if we are limited to commenting only on the privacy implications of an AI application, the fact that we have reviewed, commented on, or even investigated the privacy aspects of such an application can give the impression that the AI application has “passed” and that it’s now safe or wholly beneficial to society. In reality, an AI system that uses personal health information may be in full compliance with privacy law, yet be horribly damaging to individuals, to specific groups, or to the public at large, for reasons not directly connected to privacy. It is not uncommon for us to give feedback, formally or informally, to custodians of personal health information, about a privacy impact assessment, and if that feedback is largely positive, it is used to promote the project as having met OIPC standards. The worst case scenario for us would be to see a harmful AI program launched about which decision-makers and the public have been told it “passed” our review process, so any subsequent critiques on ethical grounds are spurious. Without the ability, within the scope of our mandate, to comment more broadly on an AI application, it is indeed possible that our review of the privacy considerations could actually cause more harm than good.

In June 2022, the federal government tabled the *Artificial Intelligence and Data Act (AIDA)* as part of Bill C-27, which at the time of writing, has still not been passed by Parliament. *AIDA* is a first generation effort to regulate AI in the public interest, and it contains many important provisions that will significantly impact how AI-enabled products and services are developed and made available for use by Canadian businesses and the general public.

While there appears to be an intention with *AIDA* to regulate “high-impact” AI systems, it is not yet clear how effective the implementation and oversight of this statute will be. By way of comparison, the Federal Privacy Commissioner has limited presence at the local level in this jurisdiction. It rarely issues investigation reports into matters involving this jurisdiction. Its resources are finite, and it is often involved in investigating matters involving major national and multi-national corporations and in providing leadership on privacy matters of national scope and importance. Given that the new data commissioner, under the current *AIDA*, will not be an officer of Parliament but rather report directly to the Minister whose job it is to foster the development of the AI industry in Canada, it cannot be assumed that any AI applications in the health sector in this province will have been vetted by the data commissioner or will be in compliance with the requirements of that office, any more than every video surveillance camera installation has been considered by the federal Privacy Commissioner. Furthermore, it also cannot be assumed that the “high impact” criteria in *AIDA* will necessarily mirror closely the statutory requirements of *PHIA*. In addition, the ethical implications of broader societal impacts under *AIDA* will only be considered in light of the current protected grounds of discrimination under the *Canadian Human Right Act*, such as age, sex, gender identity or expression, etc. This is a relatively narrow, if perhaps more objectively assessed, criteria for harm beyond privacy, however it is quite limited, because something can be harmful to society more broadly, without necessarily having a discriminatory impact on the specific criteria listed in that Act.

Ultimately, we are still very much of the view that *PHIA* (and *ATIPPA*, 2015 for that matter), should both contain very basic first generation provisions addressing artificial intelligence.

Other than the definition issue addressed above, we repeat the same recommendations we made to Chair Orsborn of the 2020 ATIPPA review, which, adapted for *PHIA*, are:

- Incorporate a definition of artificial intelligence into *PHIA*.
- Require algorithmic assessments to be conducted by any custodian prior to implementation of a program involving the use of artificial intelligence. Custodians must also ensure that this requirement is designed into any agreement with an information manager or agent who is carrying out work on behalf of the custodian and using personal health information that is in the control or custody of the custodian.
- Require a custodian intending to develop and implement a program involving the use of artificial intelligence to notify the Commissioner of that intention and engage the Commissioner at an early stage of the development of that program, including providing to the Commissioner a copy of an algorithmic assessment for review and comment by the Commissioner prior to implementation of the program.
- In addition to privacy and access to information issues, in its review and assessment, the OIPC should be entitled to comment on all implications for the use of AI in the proposed program, including data ethics factors such as proportionality, fairness and equity, in a manner comparable to a data commissioner; to this end, amendments to the purpose of *PHIA* may be required to reflect the added mandate for an independent oversight agency that is empowered to review and comment on the implications, including privacy and data ethics implications, for the implementation of artificial intelligence in a custodian's programs. Comparable powers or duties should be added to section 79.

Custodianship

The 2016 Statutory Review focused on this topic at some length so it is not necessary to repeat the discussion here, but it is important to draw attention to a couple of general principles: that the custodian is the entity that should be responsible for safeguarding personal health information and where two entities are responsible for the same thing, then the risk is that no one is responsible for it. Attention should be given to identifying where circumstances can arise where there may be confusion about which of two or more parties is the custodian. This may include situations where multiple health organizations may both be involved in handling the same information – they cannot all be custodians of the same instance of the same information. Shared custodianship undermines accountability. Even where agreements are put into place, those agreements can never cover every circumstance, and furthermore, there are many discretionary decisions available to custodians about collection, use and disclosure, about which two or more custodians whose work is interconnected may disagree. Finally, there are judgment calls to be made, including what constitutes “reasonable” security of personal health information. In a shared custodianship

model, it is not enough for one custodian to simply defer to the other. There also needs to be additional clarity in situations where the custodians may be natural persons (i.e. specific health professionals) and the organizations they work for, or are associated with, are health authorities or businesses.

These comments about custodianship come at a time when the very idea of custodianship as a fundamental principle of personal health information statutes has been subject to some criticism. The Expert Advisory Panel on a pan-Canadian Health Data Strategy, of which Commissioner Harvey was a member, took the position that the principle of custodianship was a hold-over from a time when health information systems were primarily paper based and the primary concern was maintaining security and introducing basic access and correction rights while ensuring access to that information by clinicians who are part of the circle of care. In an age in which health information is digital, the sector is much more data rich, and the innovation imperative is greater, health information legislation needs to be reconceived in a more sophisticated way that puts a greater focus on access and use of the information. First and foremost, the data must be more accessible by the individual to which it pertains, and not just accessible but *controllable*. In short, health information systems need to be more person centric. Second, the use of this data by other authorized parties for the public good – research, quality improvement, evaluation and innovation, should not be an afterthought but a clear purpose of the legislation.

The concept that has emerged to try to capture these ideas is to shift from a custodian based statute to a stewardship based statute. However, it is too early in the emergence of these ideas to develop a full legislative framework for them. It will likely be the next statutory review before we understand how to accomplish this. But in the interim, preparatory steps can be made for this transformation by giving attention to the purpose section of the Act to:

- Reference person centricity as the guiding principle in this access, correction and privacy statute.
- elevate the idea that the framework (which already exists) for use of data by authorized users for research, QI, evaluation and innovation .

Research and other Secondary Uses

Since *PHIA* has come into force we've seen an evolution in policy and procedure development in relation to reviewing and processing requests for access to data for research purposes, which has largely been positive. We believe that further efficiencies and benefits can be unlocked through the development of a statutory framework in *PHIA* for a provincial secondary use committee. Such a committee could review all secondary uses in terms of privacy principles, statutory compliance, and ethics, as similar committees at Eastern Health and NLCHI have done in the past. All secondary uses, including research, and especially research for commercial purposes, should be subject to review and approval by this committee, with clear direction that the Minister cannot override a decision of the committee. As it currently stands, the Minister has broad authority to direct NL Health Services per the *Provincial Health Authority Act*. Note, we are not of course contemplating a scenario in which the Minister might

compel NL Health Services to do something contrary to *PHIA* – the *Act* itself contains prohibitions about that. We are instead concerned about a situation where the Minister might be faced with political pressure to direct it to exercise its discretion in a way that varies from the advice of its internal privacy and ethics officials or the decision of a provincial secondary use committee, if indeed this recommendation is accepted. At a time when more and more personal health information is being collected about the people of the province, and when there is an increasing interest by all manner of third parties to get access to it, such a move would give the people of the province comfort that decisions about their data – much of it collected on the basis of implied consent – are being made impartially and dispassionately.

A further recommendation in relation to research is that a statutory regime for commercial research involving genetic and genomic data be developed separate from but compatible with *PHIA*, which would ensure that genetic and genomic data of Newfoundlanders and Labradorians is made available for research purposes only in ways that are of primary benefit to the people of the province, that are ethically sound and privacy protective, and that the information may only be accessed for research purposes in such a way that it remains within the legal jurisdiction of this Province.

Custodianship and Memorial University

Probably the single most contentious issue of the last *PHIA* review was the issue of custodianship and Memorial University. Perhaps a good starting point is to note that since *PHIA* came into force in 2011, the Faculty of Medicine, the School of Nursing, the School of Pharmacy, and the School of Human Kinetics and Recreation, have all been custodians in accordance with section 4(1)(j). The issue is that Memorial has long been of the view that they should not be custodians, even though their faculty members and students do, in different circumstances, have personal health information in their control or custody. Our understanding is that these schools/faculties were identified as custodians because each of them employs faculty members who may collect personal health information during the conduct of research, and they may also be involved in the provision of health services as part of curriculum delivery. However, it is not just the direct provision of health services that is at issue here. Each of those four schools (and others, e.g. Social Work) involves researchers who have, in many instances, record level health information that they use for research. In some instances the research involves direct provision of health services (e.g. clinical trials). While Memorial has, at times, claimed that research does not involve personal health information, this is not the case.

This has been a long-standing issue. Memorial University lobbied government rather effectively in the early years of *PHIA*, to the point that a bill was drafted in 2014 which would have seen those schools and faculty de-listed as *PHIA* custodians. Just prior to its placement on the Order Paper the Department notified us of it and asked if we had any concerns. We were successful in convincing the Department not to proceed with the bill. The next major phase of debate on this issue occurred in the lead-up to the last *PHIA* review, in which OIPC and Memorial both participated, as did a number of other entities.

The [Final Report](#) of the last PHIA review, which was issued in 2017, considered all of the arguments put forward by Memorial and by this Office. Our position on the matter was primarily captured in our [supplementary submission](#). The Final Report also considered arguments put forward by other entities, such as the Newfoundland and Labrador Centre for Health Information, which said the following on page 6 of its [submission](#):

The Centre discloses data to researchers regularly as part of a secondary review process. There are tiers of trust models within the review process and researchers representing other custodians are treated with a higher degree of trust. For example, if a researcher from Memorial University requests data from the Centre, the risk associated with disclosing data to him/her is considered lower than if the data was disclosed to an unaffiliated researcher since custodians are required to protect personal health information in accordance with PHIA. If a custodian designated under PHIA, were to be delisted or if their status changed, that would impact the disclosure of data to researchers affiliated with that organization.

Eastern Health, in its [supplementary submission](#), also expressed concerns about Memorial potentially no longer being a custodian, and discussed specific scenarios in which it disagreed with Memorial's views. The Health Research Ethics Board also echoed the concerns of Eastern Health, NLCH, and OIPC on this subject in its supplementary [submission](#). No submissions by any other parties supported Memorial's view on this subject.

Ultimately, the analysis of the various positions and concerns put forward on this issue found in the 2017 PHIA Review Final Report largely dismissed Memorial's concerns and supported those of the OIPC and the other parties noted. If anything, the recommendations in the Report went further than we at the OIPC or the other parties were expecting. It recommended a much broader regime of making all post-secondary institutions custodians subject to PHIA.

Following the Final Report being made public, the Department studied the recommendations for some time, and eventually invited representatives from the various stakeholders, including this Office, to participate in discussions about the issue. By the time those discussions convened, there had been substantial turnover within the relevant leadership positions at Memorial, so there was a certain appetite to rehash all of the concerns which had already been considered in the Final Report.

Ultimately, however, the Department was able to prevail upon the parties to accept that some form of custodianship was necessary for Memorial, and the only outstanding question was whether that custodianship needed to be customized in certain ways to reflect the unique role of Memorial among other custodians. The OIPC and other stakeholders readily agreed with this approach, and a series of meetings occurred during which those issues were hammered out. It was our view at the OIPC that this issue had largely been resolved and that a path forward for custodianship at Memorial was cleared. Unfortunately no amendments to PHIA actually resulted, and in the years following, there was regular turnover within the Department in terms of the point person for PHIA, so the institutional memory of the progress that had been made appears to have largely been lost, which is deeply unfortunate. There has also

been some further turnover of key figures at Memorial. We believe there should be sufficient documentation within the Department, however, recording the consensus that was in place at the time, and other than some review of the finest details, it is our view that this matter should be settled once and for all in accordance with the findings (although not the exact recommendations) of the last *PHIA* review.

Registries

Section 39(4)(d) of *PHIA* requires custodians to disclose personal health information 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.” We made recommendations on pages 23 and 24 of [our initial 2016 PHIA review submission](#) that the process of registry designation needs to be clarified. Our recommendations were echoed by others as well, and we made some additional comments in our supplementary submission:

NLCHI's comments with regard to registries created under section 39(4)(d) are consistent with those raised in the OIPC submission. NLCHI proposes that a process for designating a registry be spelled out in PHIA or in the Regulations. This Office, along with the Department of Health and Community Services, has invested a significant amount of time in working towards a viable process for doing so, and we would be pleased to see it reflected in the regulations.

It must be observed that, currently, any registries operating in the Province are operating in non-compliance with PHIA and thus are in violation of the law, because none have been formally designated by regulation. It was expected after initial proclamation of PHIA that all registries would be appropriately designated within a reasonable period of time, however this did not occur. This state of affairs regarding registries cannot be allowed to continue. The current process must be formalized, and registries must be designated.

Of crucial importance is that there must be a process for either the Minister or the Commissioner (as is the case in Ontario) to review, at defined intervals, the operation of each registry, to ensure that it continues to operate as intended, and that if there is to be any expansion of the mission or function of a registry, that any such proposed new mandate be subject to appropriate scrutiny from a privacy perspective. The fact that registries amass a huge amount of personal health information on a mandatory basis without consent must not be forgotten in the course of moving forward with the laudable public health goals facilitated by registries.

Since the last *PHIA* review, the Cancer Care Registry and the Chronic Disease Registry have been designated in the regulations, and the process of engagement between stakeholders and this Office has been positive, however it can only be considered an informal process without any regulatory underpinning, and there is no assurance that it will be continued if future registries are designated. Furthermore, it is unknown how many additional registries

even exist. Anecdotaly there has been discussion and debate about what actually constitutes a registry for the purposes of this provision, and this confusion has not been helped by the lack of a definition in *PHIA*.

Substantially Similar

One important consideration for *PHIA* review is the relationship between federal privacy law and an updated *PHIA*. Currently, *PHIA* has been deemed by Innovation, Science and Economic Development (ISED) Canada (formerly Industry Canada) as “substantially similar” to *PIPEDA*. This is important because *PHIA* regulates the collection, use, and disclosure of personal information within both the private and public sector. Private sector regulation of privacy would normally fall solely within the jurisdiction of federal regulatory authority, however because of the Canadian health care model which has both private and public sector involvement, and the interconnected nature of health care as a practice and therefore the interrelatedness of personal health records, there has been a consensus that the most practical model is a single statute in each jurisdiction that covers personal health information, whether that information is in the private or public sector. Any consideration of amendments resulting from *PHIA* review must assess whether it is necessary or desirable to retain the current substantially similar status, whether it is necessary to assess it against the current *PIPEDA* or the entire pending Bill C-27, or parts thereof. If it is deemed necessary or desirable to retain substantially similar status, it is proposed that contact be initiated with ISED to discuss the provisions that would be necessary in a future version of *PHIA* in order to retain that status. Given the very significant differences between *PIPEDA* and C-27, if *PHIA* is to be substantially similar to C-27 it could require a number of substantial amendments.

Appendix D

The Right of Privacy for Minors - Medical Records

Maintaining the privacy of health information for minors is an essential element of ensuring young people in this province have confidence and trust in their own healthcare management. The laws and policies in this Province have been the same for decades and have created the necessary balance between privacy of minors and parental involvement in medical decision making. The introduction of CorCare has allowed individuals online digital access to their medical records and that of their minor children. A debate has now arisen about the proper age where a minor can assert autonomy over their own personal health information. It is a difficult debate given the myriad of factors and opinions that inform the care of the most vulnerable of our population. It is OIPC's position that the ability of care providers to have confidential interactions with minors and have their medical records remain private is essential in providing healthcare. Children have a right to privacy and should have a say if and when a parent or guardian can access their health information once they achieve capacity to understand their decisions.

When discussing the issue of mature minors and parent/guardian rights, it is important to remember that PHIA is a law that establishes a foundation. It must protect vulnerable children and youth and ensure that medical information is shared with only the necessary people in a timely fashion. The law cannot be too prescriptive, as there will always be unique situations, and our children must continue to have their medical information protected from adults who may cause them harm.

It must be remembered that PHIA is about personal health information, not access to treatment. For example, a minor may decide to restrict a parent or guardian's access to their health record, however still welcome them to attend medical appointments with them and speak with their care teams. Further, PHIA authorizes, and sometimes requires, disclosure in specific circumstances, including when health and safety are at risk. It is our position that there are already checks and balances within PHIA that recognize extraordinary circumstances.

[Section 7](#) of PHIA establishes the rights of representatives, including the parent or guardian of a minor, stating:

7. A right or power of an individual under this Act or the regulations may be exercised

...

- (d) by the parent or guardian of a minor where, in the opinion of the custodian, the minor does not understand the nature of the right or power and the consequences of exercising the right or power;

Subsection 7(d) establishes right of the parent or guardian of a minor where, in the opinion of the custodian, the minor does not understand the nature of the right or power and the consequences of exercising the right or power. This section requires two distinct considerations. First, custodians should satisfy themselves that the parent or guardian are in fact who they say they are and have rights vis-à-vis the minor in question. Second, custodians should assess whether the minor understands the right or power under the Act that is under consideration (for example, whether to file a privacy complaint or make an access/correction request). If the minor understands, then presumably they can and should exercise the rights or powers themselves unless exceptional circumstances exist.

The purpose of the Act is stated in section 3:

3. The purposes of this Act are

...

- (b) to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in this Act;

When it comes to minors, parents and guardians have an important role to play helping minors learn to manage their health. They can learn about making informed decisions and supporting their well-being.

There are additional sections of PHIA that impact the decision-making process regarding disclosure by a custodian.

- 6(2) A provision of this Act that permits a custodian to disclose personal health information about an individual without the consent of the individual

- (a) does not compel the custodian to disclose the information unless otherwise required to do so by law;

...

- (c) does not prevent the custodian from obtaining the individual's consent to the disclosure.

These are important considerations when considering access by representatives. Custodians **may** disclose without consent, however there are narrow circumstances defined in law that **requires** them to disclose without consent. It also reminds custodians that nothing prevents them from seeking the minor's consent.

There are safeguards already in place in PHIA that consider harms that may result from disclosure, such as

- 58. (2) A custodian may refuse to permit an individual to examine or receive a copy of a record of his or her personal health information where ... (d) granting access could reasonably be expected to (i) 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, ...

Over the years, OIPC has been asked for guidance on this matter. Some key considerations in each matter can include:

- The nature of the information being requested. There is a difference between confirming when they had a particular test done versus the results of a test, for example.
- Why the clinician decided it was appropriate to disclose the information. The clinician likely has relevant knowledge. Has the minor been attending appointments alone? Is the minor able to discuss their own health and ask questions during interactions? Do they appear to understand what is going on?
- What discussion on confidentiality or notice regarding same was used at the time of the collection. What would a reasonable person consider reasonable in the given circumstances?

- A number of reports from other Commissioner's offices¹ address making access requests on behalf of someone else and assessing if the representative is acting for the minor or in their own interests. Four key considerations are:
 - Is the applicant the minor's parent or guardian?
 - Is the applicant acting "for" the minor?
 - Is the minor "incapable of acting" under section 7?
 - Is exercising the minor's rights under PHIA "within the scope of the parent or guardian's duties or powers"?
- If the minor understands the right or power of access to personal health information and the consequences of exercising the power, an argument could be made that the custodian should only release information to the minor and not their representatives (parents or guardian). This would be especially true if they had informed their clinician that they do not want their parents to know something (consent directive).

Who is a minor under Newfoundland and Labrador legislation?

The [Age of Majority Act](#) establishes that individuals cease to be minors when they turn 19, stating:

2. Every person who attains the age of 19 years
 - (a) attains the age of majority; and
 - (b) ceases to be a minor person.

The [Human Tissue Act](#) supports an individual's ability to make decisions regarding the donation of body tissue starting at the age of 19, stating:

4. (1) A person who has reached the age of 19 years, is mentally competent to consent, and is able to make a free and informed decision may, in writing signed by him or her, consent to the removal from his or her body of the tissue specified in the consent and its implantation in the body of another living person.

¹ See, for example, [Order F17-04](#) from OIPC BC.

While the [Children, Youth and Families Act](#) does not define the term minor, it does define child and youth in section 2, stating:

(d) "child" means a person actually or apparently under 16 years of age;

...

(ff) "youth" means a person who is at least 16 years of age but under 18 years of age.

This Act also contemplates medical treatment, acknowledging that there may be circumstances where a child is in need of protective intervention because of a refusal or failure to obtain or permit essential medical treatments recommended by a qualified health practitioner. This suggests that some parents or guardians may not be acting in the best interests of a minor and should therefore not have blanket rights on access to information and/or medical decisions.

Finally, section 92(1) states that, “A person over 12 years of age has the right to and shall, on request, be given information relating to himself or herself.”

Canada Health Infoway Report

In 2016, Canada Health Infoway released a report, [Provisions Relating To Minors in Provincial and Territorial Health Information Privacy and Health Care Consent Statutes](#). OIPC NL asked jurisdictions if anything had changed since this report was issued. While not all jurisdictions responded, a number provided additional information.

Quebec

Quebec’s [Act respecting health and social services information \(chapter R-22.1\)](#), passed in 2024, uses 14 as the key age. The Québec Health Booklet, [Carnet santé Québec](#),² provides online access to an individual’s personal health information. The health record of any child under the age of 14 is automatically linked to their parents' records. Children aged 14 or older must log in to Carnet santé Québec themselves to access their health information. Health

² Link may be blocked on some gov.nl assets

information—such as test results, medications, and medical imaging reports—is not accessible in children's records as of July 2026.

Another aspect of the Quebec legislation is that parents or guardians of a minor aged 14 or older are not notified that the child has received care required by their health condition, unless the minor stays in a health or social services facility for more than 12 hours; in that case, the parents or guardian will be notified that the child has been admitted to the facility.

Alberta

In Alberta, the Ministry responsible for implementing the provincial patient portal established a process to determine if a minor (under 18) can access their information in the system. Initially, this involved having a qualified professional assessing a minor and determining if they could be considered a mature minor. Considerations included age, intelligence, maturity, the seriousness of the health care related decision, informed consent, and freedom from parental or guardian control, self-supporting, married or has children.³

Recent changes have impacted the above process. Alberta now allows children to be active in managing their personal health information starting at age 14, when they can register for their own MyHealth Alberta Account. At 16, they may choose to remove previously granted parent/guardian access and at age 18, parent/guardian access ends automatically.⁴

Key notes:

- Parents/guardians can submit an online request to access personal health information when their child is younger than 16 years of age. Requests for children 16 and older would need to be discussed with the child's Regulated Health Care Provider. Regulated Healthcare Providers can add or remove access to a child's personal health information upon request.

³ [Minors/Mature Minors Summary sheet](#)

⁴ [Parent/Guardian Access](#)

- Parents of minors 14 years of age or older that already have a MyHealth Alberta Account cannot obtain access through the online request tool. They need to ask a regulated health care provider for access.

British Columbia

While British Columbia has two pieces of legislation to consider, it is one of the few jurisdictions without health sector specific legislation. This complicates the discussion of mature minors, as either the [Freedom of Information and Protection of Privacy Act](#) (FIPPA) or the [Personal Information Protection Act](#) (PIPA) applies. PIPA is a private-sector law that is consent-based, while FIPPA is a public sector law that is not consent-based.

[Section 5](#) of FIPPA and [section 23](#) of PIPA set out general information access rights (for all individuals, including minors) and the regulations establish the rules about when a guardian can access records on behalf of a minor:

- [Section 3 of FIPPA Regulation 155/2012](#) specifies that a guardian can only act for a minor to access their information “if the minor is incapable” and if it is “within the scope of the guardian's duties or powers”.
- [Section 2 of the PIPA Regulations](#) specifies that a guardian can only exercise the rights of the minor under section 23 of the Act “if the minor is incapable of exercising the minor's rights under that section”.

Consent is required for most collections, uses and disclosures in PIPA and OIPC BC published joint guidance on [Obtaining Meaningful Consent](#) with OIPC Alberta and the Office of the Privacy Commissioner of Canada. Discussion on children and consent is on page 10 and states, in part:

The OPC is of the view that while a child’s capacity to consent can vary from individual to individual, there is nonetheless a threshold age below which young children are not likely to fully understand the consequences of their privacy choices, particularly in this age of complex data-flows. ...(the OPC takes the position that, in all but exceptional circumstances, this means anyone under the age of 13), ...

Saskatchewan

Saskatchewan's [Health Information Protection Act](#) (HIPA) establishes situations when others can exercise the rights of individuals. Two sections specifically address circumstances when these rights could be exercised by minors or guardians or minors stating, in part:

56 Any right or power conferred on an individual by this Act may be exercised:

...

- (c) by an individual who is less than 18 years of age in situations where, in the opinion of the trustee, the individual understands the nature of the right or power and the consequences of exercising the right or power;
- (d) where the individual is less than 18 years of age, by the individual's legal custodian in situations where, in the opinion of the trustee, the exercise of the right or power would not constitute an unreasonable invasion of the privacy of the individual;

When it comes to online access to a minor's health record, eHealth Saskatchewan has established a process for Parents and legal guardians to request access to health information in MySaskHealthRecord for children under age 14.⁵ A [form](#) must be completed that contains the following note,

The definition of a person who is legally responsible for the care and custody of the minor may not extend to the biological parents of a child in all circumstances. A court order or agreement between the biological parents can give custody to only one of the biological parents. A child could also have other guardians who are not biological parents such as a child's grandparent or other relative or other individual who has been granted a guardianship order by the Court. eHealth therefore must take reasonable steps to ensure the applicant is the legal guardian of the child and one of those steps is to request legal documentation related to the legal custody of the child in question.

By the signature line, the form also informs individuals that it is an offense under HIPA to obtain another person's personal health information by falsely representing that you are entitled to the information; this could result in a fine of not more than \$50,000, to imprisonment for not more than one year or to both.

⁵ [Accessing MySaskHealthRecord on behalf another individual | eHealth Saskatchewan](#)

Conclusion

- The impact of online digital access to our medical records has raised privacy and access issues for minors that did not exist previously. In the past, parents, healthcare providers and minors worked together to ensure access was provided or limited where appropriate given the specific situation of the minor. There are families where access is entirely appropriate and should continue, but there are also situations where parental access is absolutely inappropriate. As each case has individual factors, it makes sense that the healthcare provider make those assessments and act in the best interests of the minor. To set a hard age where parents must always have access to medical records fails to take into account the confidentiality that may be necessary to protect the minor who has capacity to understand their own decision making. If privacy provisions for minors in PHIA are to be amended then any legislative changes must ensure that vulnerable minors continue to be protected.
- a minor's capacity or incapacity to understand their access rights must be considered; this may not be the same age for each individual.
- that minors are at minimum aware of who has access to their record and, in practice, it is preferable that they have a say in who has access to their record.
- consent directives are honoured and that minors are able to restrict access to their record and/or specific information within that record.
- the privacy, health and well-being of minors must be paramount; an unintended consequence may be that minors stop seeking medical assistance.

Appendix E

Correction and Annotation of Medical Charts Given the Accessibility of Charts by Patients in the Digital Age

Annotation has been a challenge for OIPC as well as for Custodians. OIPC has issued guidance¹ and several reports ([AH-2014-001](#), [AH-2020-001](#), [AH-2026-001](#), and [AH-2026-002](#)) that reference annotation under sections 63 and 72 of the **Personal Health Information Act** (PHIA). This submission recommends that the statutory review committee consider addressing identified gaps in PHIA. This Office supports amendments to address these gaps to provide clarity, informed by comparable provisions found in other Canadian jurisdictions.

Issue 1 - Section 63

PHIA establishes a statutory framework through which individuals may request correction of their personal health information. Where a custodian refuses to make a requested correction, PHIA requires the disputed information to be annotated. The purpose of annotation is to preserve the integrity of the original record while ensuring that those who subsequently rely upon the disputed information are aware that its accuracy or completeness has been challenged and what correction was requested. PHIA protects professional opinions from being rewritten simply because an individual disagrees with them. However, that protection must operate alongside an effective mechanism for recording the individual's disagreement. At issue is the lack of clarity and legislative gaps pertaining to annotation.

In Report AH-2026-001, the Commissioner was required to address the fact that PHIA does not set any limits on the form or content of an annotation. The Act simply states that the custodian must, “annotate the personal health information with the correction that was requested and not made”. As seen in this case, a request for correction may be lengthy and difficult to interpret, and it may include extraneous information and opinions or perceptions that go beyond what would normally be necessary or appropriate in a correction request. A superficial reading of PHIA would require a custodian to take the entire correction request and add it to the patient's medical record as an annotation, which may not be reasonable, practical, or in the best interest of the patient or custodian. Although the Report adopts an

¹ There is a section regarding annotation and correction in our [PHIA Toolkit for Small Custodians](#) at pages 13-15.

interpretation of the language in PHIA in an attempt to apply some limitations in cases such as this, clearer statutory language would benefit both patients and custodians.

A recent Report AH-2026-002 by our Office found that where a custodian refused a request for correction, an annotation must be made. In that case, the corrections requested were very numerous and impractical to fully reproduce as an annotation to the record, which a strict reading of PHIA requires. The Commissioner was able to craft a way forward, however in doing so it was observed that PHIA is lacking in some crucial elements.

Other Canadian jurisdictions have addressed the same issues through statutory provisions in comparable Acts that provide sufficient clarity regarding annotations, including the purpose, content, reasonable length, and proximity to the health record in dispute.

- Alberta - [Alberta Health Information Act](#) section 14(1)(b) deals with a Custodian's refusal to correct or amend. It provides a "500 words or less" limit within the Act. It also differs in that it refers to a statement of disagreement versus annotation. Alberta Order [H2009-001](#) is especially useful as it addresses a 500-word standard, and extraneous material.
- Ontario – [Personal Health Information Protection Act, 2004 s. 55\(11\)\(a\)](#) requires that a statement of disagreement (the Ontario version of an annotation) be "concise". In [PHIPA Decision 162](#) the Adjudicator found that the correction requested by the Complainant did not meet the requirements of a statement of disagreement as it was not "concise". This was based on the fact that it contained extraneous information. [PHIPA Decision 236](#) made a similar finding that the Complainant's statement of disagreement did not meet the requirement to be "concise" under the Act as it contained "a number of allegations and statements that go well beyond a concise statement of disagreement". The Senior Adjudicator also noted that the Complainant had the right to make a complaint to the IPC for a determination of if a new statement of disagreement met the requirements set out in the Act.

Recommendation

It is recommended that the following amendment be made to section 63(2)(a) of PHIA:

63(2) Where a custodian refuses to grant a request for correction under paragraph 62(1)(b), he or she shall

- (a) annotate the personal health information with the correction that was requested and not made or a reasonable and concise summary thereof, and, where practicable, notify a person to whom the information was disclosed within the 12 month period immediately preceding the request for correction of the notation unless the custodian reasonably expects that the notation will not have an impact on the ongoing provision of health care or other benefits to the individual or the individual requesting the correction has advised that notice is not necessary; and

Issue 2 - Section 72

A related issue is that section 62 permits a custodian to refuse a requested correction and where a correction is refused, section 63 dictates the personal health information must be annotated with the correction that was requested and not made. Section 72 authorizes the Commissioner to recommend a Custodian make a requested correction. However, a gap exists in section 72 whereby the Commissioner does not expressly have the authority to recommend that an annotation be made.

[Report AH-2026-001](#) exposed a deficiency in the recommendations section of the Act. Section 72(2)(b) authorizes the Commissioner to recommend the Custodian make the requested correction. The Act does not provide a corresponding authority to recommend that a Custodian make an annotation compliant with section 63(2). As the general legal principal says, where there is a right there is a remedy. This Office has interpreted section 72(2)(c)(iv) to be broad enough to allow for a recommendation that, in this case, the Custodian implement an information practice of annotating the Complainant's medical record with the amended annotation, as it is reasonably necessary to achieve compliance with the Act. Engaging section 72(2)(c)(iv) in Report AH-2026-001 was a solution to an omission in the Act, where an information practice is reasonably necessary to achieve compliance. Most significantly, while a recommendation under 72(2)(b) provides a path to court for further appeals, section 72(2)(c) is purely ombuds in nature. The result is that a complainant who has had a correction

refused may go to court subsequent to the issuance of a Commissioner's report, however a complainant who has had an annotation refused may not.

Additional inconsistency exists currently within the Act whereby the Trial Division has express authority under 86(c) to order a Custodian to Correct or Annotate while 72(2)(b) addresses correction only.

Recommendation

It is recommended that the following amendment be made to section 72(1)(b) of PHIA:

Where the review relates to a complaint respecting a refusal to correct a record of personal health information,

- (i) recommend that the custodian make the requested correction;
- (ii) recommend that the custodian annotate the personal health information with the correction that was requested and not made, or a reasonable and concise summary thereof.

Appendix F

Information and Privacy Commissioner,
Ontario, Canada



Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PI21-00001

McMaster University

February 28, 2024

Summary: The Office of the Information and Privacy Commissioner of Ontario (the IPC) received a complaint about McMaster University's (McMaster or the university) use of Respondus exam proctoring software under the *Freedom of Information and Protection of Privacy Act* (FIPPA or the *Act*). The software comprises two programs. Respondus LockDown Browser limits what users can access on their computers and Respondus Monitor analyzes audio and video of students during the exam to scan for possible cheating. The complainant did not want the IPC to provide their name and complaint to the university, so the IPC opened this Commissioner-initiated complaint to address the university's use of this exam proctoring software.

This report concludes that conducting exams and appointing examiners is a lawfully authorized activity of the university. Proctoring exams online to ensure their integrity is an appropriate component of conducting certain types of exams and is therefore also a lawfully authorized activity. On the question of whether the collection of personal information through the use of Respondus exam proctoring software is necessary to proctor exams, I find that Respondus LockDown Browser collects little personal information, and only collects and uses what it needs to function. Respondus Monitor collects more sensitive personal information, including biometric information, and uses artificial intelligence (AI) technology, which carries heightened concerns. Because the personal information collected by Respondus Monitor on behalf of the university is necessary for that tool to fulfill its function of exam proctoring, it is authorized under section 38(2) of the *Act*. However, the university has not provided adequate notice for its collection of personal information as required by section 39(2) of the *Act* and the use of students' personal information through Respondus Monitor is not in compliance with section 41(1). Moreover, the

current contractual arrangement between the university and Respondus is contrary to section 41(1) of the *Act* in so far as it does not adequately protect all of the personal information collected and allows Respondus to use personal information for system improvement purposes without the consent of students.

In this report, I make a number of recommendations for the university to bring itself into compliance with the *Act*. Given the heightened risks associated with AI technologies, I also recommend that the university adopt additional guardrails around its use of Respondus Monitor and incorporate these stronger protections into its ongoing use of the software and any future agreement with Respondus.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990; R.R.O. 1990, Regulation 460; *McMaster University Act*, 1976

Orders and Investigation Reports Considered: Investigation Report 196-057M and Privacy Complaint report PR16-40.

Cases Considered: *Cash Converters Canada Inc. v. Oshawa*, 2007 ONCA 502.

BACKGROUND:

[1] In January 2021, the Office of the Information and Privacy Commissioner of Ontario (the IPC or this office) received a complaint from a student at McMaster University (McMaster or the university) regarding its use of proctoring software for exams conducted remotely and online. The software being used was Respondus LockDown Browser and Respondus Monitor, both from the vendor, Respondus.

[2] The student raised concerns that McMaster was inappropriately collecting student data via this software and was unsure how the university was using, disclosing and disposing of student personal information gathered via this software.

[3] The student did not consent to the IPC sharing their name and a copy of their complaint with the university. As such, the student's complaint file was closed and this Commissioner-initiated file was opened to address the university's use of proctoring software.

[4] The complaint was brought in January 2021 during the height of COVID-19 related restrictions.¹ The university stated that it began using Respondus Monitor and Respondus Lockdown Browser to administer remote assessments in 2020, the first year of the COVID-19 pandemic. McMaster continued to hold classes virtually through the bulk of 2021², with 50% of course components returning to on-campus attendance as of

¹ See, for example, the additional emergency measures put in place on January 13, 2021: <https://news.ontario.ca/en/release/59922/ontario-declares-second-provincial-emergency-to-address-covid-19-crisis-and-save-lives>

² <https://covid19.mcmaster.ca/spring-summer-and-intersession-2021-terms-to-be-held-virtually/>

September 2021.³ The Omicron wave caused a temporary reversion to remote learning for a brief time between December 2021 and January 2022.⁴ However, as of January 31, 2022, Ontario's phased re-opening plan saw restrictions begin to ease.

[5] Respondus Lockdown Browser and Respondus Monitor programs are often used together, though Respondus LockDown Browser can be used on its own.

[6] Respondus describes Lockdown Browser as a custom browser that locks down the testing environment within a learning management system.⁵ The user must install this software, and when in active use it displays the assessment full screen and locks some functions of a student's computer to discourage cheating. During assessments, students are unable to conduct an internet search, access files on their computer, navigate away from the assessment screen, or use the copy-paste, messaging, screen sharing, or print screen functions. Lockdown Browser does so by making changes to local settings on students' computers to temporarily control or restrict access to computing resources.

[7] Respondus Monitor accesses a student's webcam and records them during assessments, acting as a form of virtual invigilation. The recordings, including biometric information, are analysed using artificial intelligence (AI) to flag activities it deems suspicious or consistent with cheating. Instructors are provided with a report of flagged events for their review. The inclusion of a suspicious activity flag does not necessarily mean that the student was cheating. Instructors may request to review the exam recording via McMaster's Academic Integrity Office and speak to the student to assess whether there was potential academic dishonesty that should be referred as a possible breach of McMaster's Academic Integrity Policy.

[8] On July 17, 2020, McMaster publicly released "Privacy & Information Security Impact Assessment Report – Online Proctoring: Respondus"⁶ (PIA Summary) which provided background, analysis, and key findings and recommendations from this assessment report.

[9] In that PIA Summary, McMaster outlined the challenges of the COVID-19 public health emergency, including its resulting inability to deliver in-person examinations with proctors or invigilators. While some instructors were able to use existing tools to conduct exams or other evaluations, the university noted that these solutions were unlikely to fill the needs for all courses, including accredited courses. To address this gap, the university launched a pilot project and evaluation of online proctoring options to find a preferred approach for fall 2020. The PIA Summary notes that the university conducted a preliminary risk assessment of Respondus in June 2020, followed by an In-depth Risk

³ <https://provost.mcmaster.ca/app/uploads/2021/09/McMasterU-Continuity-of-Education-Plan-2021.pdf>

⁴ <https://president.mcmaster.ca/mcmaster-community-december-2021/>

⁵ <https://web.respondus.com/he/lockdownbrowser/>

⁶ <https://secretariat.mcmaster.ca/app/uploads/PIA-Report-Online-Proctoring-Respondus.pdf>

Analysis later that same month. Based on the key findings and recommendations in that PIA Summary, McMaster contracted with Respondus to provide online proctoring for exams.

[10] Among the key findings of the PIA Summary were that individual students should be able to make arrangements if they require an accommodation, and that Student Accessibility Services should have an opportunity to identify those accommodation requirements to the service provider. The PIA also indicated that the application must only be installed for the duration of the exam and may be removed afterwards, and that for courses using Respondus, the course outline should clearly communicate its use to students.

[11] Also pursuant to the PIA Summary, McMaster made arrangements for students to access Respondus through the University's Avenue to Learn portal, rather than requiring students to create individual accounts to access the software. This dispensed with the collection of students' individual contact information by Respondus.

[12] McMaster set out three separate criteria for the use of Respondus software, which apply to both Respondus LockDown Browser and Respondus Monitor:

- The course is accredited;
- The course is mandatory; or
- The class size and/or assessment method dictates its use.

[13] I note that the criteria above do not include the presence of COVID-related restrictions. Under these parameters, McMaster allows the continued use of Respondus LockDown Browser and Respondus Monitor post-pandemic as long as one of the three conditions is met.

[14] Regarding the first condition, McMaster notes that accreditation is determined by a third party where a course or program must meet certain standards to satisfy professional and regulatory requirements. Proctored invigilation may be one of the conditions set out for such a course. McMaster offers a range of accredited programs, including nursing, psychology, rehabilitation, social work and engineering. McMaster states proctored exams may be a requirement for professional certification in these fields.

[15] Regarding the second condition, McMaster notes that only some courses are mandatory to obtain a degree; others are elective. Assessments for mandatory courses are identified as essential assessments and are eligible for Respondus use.

[16] Finally, regarding the third condition, McMaster has determined that Respondus may be used based on the nature of the assessment required, or the size of the course itself. Courses that have a large class size are eligible for online proctoring, as are those that require person-to-person assessment, such as languages.

[17] McMaster, on its own behalf and through its associated MacPherson Institute, has provided guidance to instructors who are considering using Respondus software. The guidance provides in part as follows:

Respondus monitors students while they are completing online assessments with an aim to ensure academic integrity. However, the decision to use Respondus should not be taken lightly. Please ensure you have considered the following:

- Rationale: do you really need to use online proctoring? Unless a proctored assessment is a requirement for a professional certification, you should consider alternate assessments or, if you rely on quizzes and tests, refer to our Guide to Tests and Exams Using Avenue to Learn on how you can configure tests and quizzes to increase fidelity without having to use a proctoring technology.
- Communication: have you included a statement as to your rationale and use of online proctoring in your course syllabus? Will you ensure instructions on how to use are provided to students along with a practice quiz?
- Accommodation: Quizzes that use Respondus can be configured on Avenue to Learn for accommodation purposes, but you will also need to develop a Plan B for certain accommodations or if technical/connection issues arise.
- Mental health and well-being of your students: consider the added layer of anxiety online proctoring can promote and how to support students through this.⁸

[18] The university also recommends that instructors explore other alternatives to proctored exams, including take home exams, projects, reflections, group work, guided online discussions, and peer-reviewed activities.

[19] If an instructor wishes to use Respondus software, they must apply in advance to use these tools in their course. The application must identify which service they wish to

⁸ <https://mi.mcmaster.ca/respondus/>

use and provide a rationale for this use. The instructor must also confirm that they have notified their students of their intention to use Respondus as an online monitoring tool.

[20] The responsible IT manager reviews this application. If they identify any concerns that the request falls outside the university's criteria for the use of Respondus, they are to consult with the privacy office and provost's office on the matter.

[21] In its online FAQ⁹ directed to instructors, McMaster addressed how Respondus software works, information about the flags in the post-exam reports provided to instructors, and what instructors should do in such instances. In addition to the information provided on its website, McMaster states that it informed instructors of the availability and limitations of the use of Respondus software via faculty channels.

[22] McMaster also provided information to students by publishing resources online, including "An Introduction to Respondus."¹⁰ This includes sections on why Respondus is being used, the data that is being collected, and the relevant privacy and data retention practices. It also directs students to additional resources if they have any concerns.

[23] "Writing a Test Using Respondus"¹¹ is another online resource provided by McMaster. It provides information on the steps to take before, during, and after a proctored exam. It also provides information regarding how the information gathered from the recordings is used by the university after the test is complete. It notes that the instructor receives a spreadsheet that summarizes any flags during the test. The instructor is to review the flags and begin a conversation with the student if there is a concern. It notes that the student's video is only reviewed by the instructor upon the instructor's request and if appropriate.

[24] This is consistent with the information that McMaster provided to the IPC. McMaster stated that instructors cannot access recordings from the exam sessions without authorization from the Academic Integrity Office pursuant to an academic integrity investigation. Otherwise, instructors do not receive copies of the recordings, and have no ability to access them.

[25] McMaster noted that since it began using Respondus Monitor in 2020, there have been two cases where recordings were reviewed as part of an investigation. The university stated that in both cases, the students were charged with academic integrity misconduct, and the recordings were integral in providing evidence documenting the misconduct. McMaster also takes the view that the use of the software generally deters students from engaging in inappropriate activity as they know their actions can be viewed.

⁹ <https://avenuehelp.mcmaster.ca/exec/respondus-lockdown-browser-and-respondus-monitor-instructor-faq/>

¹⁰ https://mi.mcmaster.ca/app/uploads/2021/03/An-Introduction-to-Respondus-_updated.pdf

¹¹ <https://mi.mcmaster.ca/app/uploads/2021/03/RESPONDUS-Writing-a-Test-Using-Respondus-Updated.pdf>

[26] McMaster has provided alternative assessments for students who have registered for academic accommodation with Student Accessibility Services. The accommodation was for assessment without artificial intelligence monitoring, in which the university provided human proctoring via Zoom for 34 students in the 2020/21 academic year, and 32 students in the 2021/22 academic year. According to McMaster, there were no accommodation requests for in-person proctoring in 2022-23.

ISSUES:

[27] The following issues have been identified as arising from this investigation:

1. Is the information at issue “personal information” as defined by section 2(1) of the *Act*?
2. Was the collection of the personal information in accordance with section 38(2) of the *Act*?
3. Is the notice of collection in accordance with section 39(2) of the *Act*?
4. Was the use of personal information in accordance with section 41(1) of the *Act*?
5. Does the university have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students, in accordance with the requirements set out in section 4(1) of Ontario Regulation 460 and sections 4(1) and 5 of Ontario Regulation 459, made pursuant to the *Act*?

DISCUSSION:

Issue 1: Is the information at issue “personal information” as defined by section 2(1) of the *Act*?

[28] McMaster was asked to describe the information Respondus collects via the students’ use of Respondus Monitor and Respondus LockDown Browser. McMaster stated that as of fall 2020, students could access both Respondus programs by logging into the McMaster “Avenue to Learn” portal, eliminating the need for students to provide individual contact information. The university separately provides the vendor with the student’s name and the course codes.

[29] During the assessment process, Respondus LockDown Browser does not routinely collect information. The exceptions are 1) when a student ends an exam session early, in which case they must provide a reason for doing so; and 2) if a student requires technical support and accesses the Respondus Help Center.

[30] At the start of each assessment session, students are required to provide photo identification, and Respondus Monitor captures this image. This software records audio and video of students throughout the exam session, which includes collection of students' biometric data.

[31] The university provided the following description of the biometric data collected:

The biometric data collected by Respondus Monitor include facial expression, body posture and positioning, direction of the test takers (sic) eye-gaze, and verbal elements. These elements are tracked and recorded to document when a student may have an unauthorized text or tool (e.g. cell phone), or unauthorized conversation regarding the answers in an assessment event.

[32] Under section 2(1) of the *Act*, "personal information" means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

[...]

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

[33] McMaster has agreed that the video recordings, course information, and biometric elements are students' personal information. I agree and find that the accompanying audio recordings should also be considered personal information.

[34] McMaster did not take a position on whether students' names, provided as part of the use of Respondus Lockdown Browser, were also personal information. I find that names, taken together with course information, are personal information pursuant to section 2(1)(h) of the *Act*. I also find that the photo identification captured by the video recording is personal information pursuant to sections 2(1)(a) and 2(1)(c) of the *Act*.

[35] In summary, I find that the students' names, course information, biometric data, photo identification, and audio and video recordings are "personal information" as defined in section 2(1) of the *Act*.

Issue 2: Was the collection of the personal information in accordance with section 38(2) of the *Act*?

[36] Section 38(2) of the *Act* prohibits the collection of personal information other than in the following circumstances:

No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

[37] McMaster has agreed that Respondus was acting on behalf of McMaster when it collected the students' personal information via the use of Respondus LockDown Browser and Respondus Monitor.

[38] When asked for the university's authority for the collection of this personal information, McMaster referred to section 13(h) of the *McMaster University Act*¹², which states that "[the] Senate has power to... conduct examinations and appoint examiners." McMaster also provided guidance documents addressing undergraduate and graduate exam policies.

[39] From this response, McMaster appears to be taking the position that the collection of personal information is either expressly authorized by statute under the second branch of section 38(2) or necessary to the proper administration of a lawfully authorized activity under the third branch of the same section. I address both these grounds.

Expressly authorized by statute

[40] Previous IPC reports have addressed what constitutes collection that is "expressly authorized by statute". In Investigation Report 196-057M, the identically worded provision of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) was interpreted as follows:

¹² *McMaster University Act, 1976*, as amended by Bill 173, Chapter 5, S.O. 2016

[In] our view, the phrase “expressly authorized by statute” in section 28(2) of the Act requires either that specific types of personal information collected be expressly described in the statute, or a general reference to the activity be set out in the statute, together with a specific reference to the personal information to be collected in a regulation under the statute; i.e., in a form or in the text of the regulation.

[41] This interpretation has been upheld and applied by the Ontario Court of Appeal in *Cash Converters Canada Inc. v. Oshawa (City)* (“*Cash Converters*”).¹³

[42] The provision of the *McMaster University Act* setting out its power to conduct examinations and appoint examiners does not address the university’s power to collect specific personal information for this purpose, and the university did not identify any regulation to this effect. Based on the information before me, I find that the collection of student personal information by Respondus software on behalf of the university was not expressly authorized by statute.

Necessary to the proper administration of a lawfully authorized activity

[43] *Cash Converters* is also the leading authority on the interpretation of the third branch of section 38(2) which I refer to as the “necessity test”. The Court’s reasons in that case make it clear that the necessity test has two requirements to be addressed separately and in the following order:

1. Is the activity engaged in by the institution a lawfully authorized activity? If the answer is “No”, the collection does not comply with the statute.
2. If the answer to question 1 is “Yes”, is the collection of the personal information necessary to the proper administration of that activity?

[44] To satisfy these two requirements, an institution must identify the lawfully authorized activity in question, and then explain how the collection of personal information is necessary to its administration.

Lawfully authorized activity

[45] As mentioned above, section 13(h) of the *McMaster University Act* sets out the university’s power to conduct examinations and appoint examiners. While this provision is the source of the university’s power, it does not represent the full scope of its lawful

¹³ 2007 ONCA 502, at paras. 36-37.

authority flowing from the power to conduct exams. Sections 78 and 79 of the *Legislation Act* expand beyond this explicit authority as follows:¹⁴

Incidental powers

78 If power to do or to enforce the doing of a thing is conferred on a person, all necessary incidental powers are included.

Performance when occasion requires

79 Powers that are conferred on a person may be exercised, and duties that are imposed on a person shall be performed, whenever the occasion requires.

[46] As explained in *Cash Converters*, a general power given to a public body by statute should be given “a broad and generous interpretation” that allows it to achieve its legitimate interests.¹⁵

[47] There can be no doubt that the university’s lawful authority to conduct examinations includes the incidental power of proctoring these exams to ensure their integrity. The question then arises whether *online* proctoring is itself a lawfully authorized activity.

[48] I am not aware of any principle of statute or common law that would confine the method by which the proctoring of examinations may be conducted by McMaster to an in-person setting, or that would lead me to conclude that online proctoring is not a lawfully authorized activity. I find that online proctoring was a lawfully authorized activity when in-person learning was not possible during the COVID-19 pandemic. Although it is now possible to resume in-person invigilation post-COVID, I accept that there may be other legitimate reasons why the university would continue to use online exam proctoring as a means of fulfilling its statutory authority to conduct examinations in circumstances that have significantly changed since the pandemic.

[49] The university has a legitimate interest in trying to ensure academic integrity by identifying and deterring cheating in exams. McMaster provided statistics showing an upward trend in academic integrity cases, with a spike in the 2020-21 academic year. The university provided an explanation for why it believed this increase had occurred:

As you can see, the Office of Academic Integrity has seen an increase in student academic integrity issues during the pandemic. This is not surprising, as other institutions are reporting the same, but it is a challenge that the university needs to address. There are a number of contributing

¹⁴ 2006, SO 2006, c 21, Sch F, ss. 78, 70.

¹⁵ *Cash Converters*, at para. [24](#).

factors including: increasing ease of online collaboration (Reddit, SnapChat, WeChat, Discord, texting), companies that facilitate contract cheating and collaboration during tests (Chegg, Course Hero); attitudinal changes in students; more online testing tools; and an increasing pressure and anxiety experienced by students. These factors have been amplified during the pandemic due to remote course delivery and increased community stressors.

[50] While the academic integrity concerns noted above may have been amplified during the COVID-19 pandemic, they are not all specific to pandemic-related conditions. I accept that by incorporating online proctoring into its evaluation methods, McMaster was also attempting to address other new challenges that arise in an increasingly digital and remote learning context.

[51] Consequently, while I accept that the inability to conduct in-person examinations during the COVID-19 pandemic was the initial impetus for McMaster adopting the Respondus software to proctor online exams, the removal of that public health limitation does not render collection unlawful at the first step of the analysis under section 38(2).

Necessary to the proper administration of the activity

[52] The next question is whether it was necessary for McMaster to collect the personal information that it did, via the use of Respondus software, for the purposes of conducting and proctoring exams.

[53] The test for determining whether this second requirement is satisfied was articulated by the Court of Appeal in *Cash Converters* as follows:

... [T]he institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not “necessary” within the meaning of the *Act*. Similarly, where the purpose can be accomplished another way, the institution is obliged to choose the other route.¹⁶

[54] I now turn to examine the functionality of Respondus Lockdown Browser and Respondus Monitor separately to determine whether the collection of each item or class of personal information was necessary for the purpose of conducting and proctoring online exams. I note that the findings below are specific to the Respondus software at issue in this case, and may not apply to other online proctoring software, which would be subject to their own analyses.

¹⁶ *Cash Converters*, at para. 40.

Respondus LockDown Browser

[55] In-person proctoring generally involves a controlled environment combined with invigilators who observe the test-takers. Similar to the controls present in an examination room, Respondus LockDown Browser works by providing a controlled environment, placing the student in a setting where they cannot easily access outside resources. Once in place, Lockdown Browser holds the computer environment secure but does not collect more than a minimal amount of the student's information, namely the student's name and course number, and certain additional information if a student ends the exam early or accesses the Respondus Help Center.

[56] I accept that the university is obliged to put such limits in place during online examinations, just as it does during in-person exams. I find that the limited personal information that the Respondus LockDown Browser collects is necessary and proportional for that purpose. Given how closely the information collected by LockDown Browser corresponds to the information provided by students during in-person exams, the University has demonstrated that LockDown Browser meets the necessity test whether exams are administered in person or online.

[57] I am therefore satisfied that the limited personal information collected on behalf of the university via the use of Respondus LockDown Browser is authorized as being necessary under section 38(2) of the *Act*.

Respondus Monitor

[58] Respondus Monitor collects a student's name and identification, as well as audio and video recordings of the student. In addition, during the examination, Respondus Monitor captures a student's biometric information in real time, including students' movements and behaviour, and analyzes this information via an AI-enabled algorithm. It then produces a report to the university which flags certain events that may indicate instances of academic dishonesty.

[59] To provide this service, Respondus Monitor has to be able to ascertain who is taking the test and collects student identification information for that purpose. Moreover, Respondus Monitor has to collect the required biometrics (which include facial expression, body posture and positioning, direction of gaze, and verbal elements) for its algorithm to assess and flag suspect behavior. Respondus also has to capture audio and video recordings of students while taking their exams to give instructors the ability to review first-hand any exam sessions which have been flagged. Otherwise, the university would not be able to provide human oversight of the algorithmic assessment, which is key to ensuring McMaster remains accountable for the use of this software.

[60] I accept that for McMaster to use this exam proctoring service, the individual items and classes of personal information collected by Respondus Monitor on behalf of the

university were technically necessary for the purpose of conducting and proctoring the exams. I am satisfied that under current law, the collection of personal information by Respondus Monitor was necessary for the proper administration of the university's lawfully authorized activity of conducting and proctoring online exams both during and post pandemic.

[61] The resumption of in person learning does not change the facts that the items or classes of personal information that Respondus Monitor collects are required for this proctoring tool to function and that Respondus Monitor collects only the information necessary for it to function. Accordingly, I find that the University's collection of personal information through Respondus Monitor is in compliance with section 38(2) of the *Act*.

Residual Concerns about the use of Respondus Monitor software

[62] To be clear, this does not mean I am unconcerned with the University's continued use of Respondus Monitor. I am keenly aware of the heightened privacy risks associated with automated online exam proctoring, as compared to in-person tests. A human proctor in an exam room observes many students in a neutral setting and does not generally record information regarding the individual students. Respondus Monitor, in contrast, is focussed on each individual student at all times, often in their home settings, potentially capturing extraneous personal information about their living environment and conditions. Through the use of its AI-enabled algorithm, it assesses whether the student may have demonstrated behaviour consistent with cheating. Respondus Monitor may "see" signs of cheating even when there is nothing there, due to the constant input of the student's movements, potential bias in the data sources used to train its algorithms, and potentially inaccurate inferences drawn from such data. This is why instructors are made aware that the report they receive may include false positives.

[63] In response to an earlier draft of this report, McMaster stated that it "retains complete autonomy, authority, and discretion to employ proctored online exams, prioritizing administrative efficiency and commercial viability, irrespective of necessity."

[64] I am troubled by the University's focus on administrative efficiency and commercial viability "irrespective of necessity", especially in the context of this type of AI-enabled technology, and the information it collects.

[65] Contrary to the University's statement, its collection of personal information in the context of online proctoring remains subject to the necessity requirement of s. 38(2). The university has statutory obligations to its students relating to the collection, use, privacy, and security of the personal information it collects and must demonstrate it is fulfilling them, regardless of any administrative efficiency or commercial advantage of any particular software.

[66] While online proctoring software must collect personal information to perform its exam proctoring function, it remains that Respondus Monitor collects particularly sensitive information. This includes biometric information and can also include background images or sounds that may provide information about the student they may not wish to share and raises risks of unfair allegations or decisions being made about them based on inaccurate information. These risks must be appropriately mitigated by effective guardrails that the university should have in place to govern its adoption and use of such technologies. In the absence of legislation regulating the use of AI in Ontario, I go on to outline what I believe some of those guardrails should be in the final section of this decision, entitled "Other Recommendations".

Issue 3: Is the notice of collection in accordance with section 39(2) of the *Act*?

[67] Under the *Act*, an institution is required to provide individuals with formal notice of the collection of their personal information. The purposes of the notice are to ensure that the institution's practices with respect to personal information are transparent and that the institution is accountable to the individual. Section 39(2) of the *Act* imposes the following notice requirement on institutions that collect personal information:

(2) Where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of,

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

[68] McMaster provided a Statement on Collection of Personal Information and Protection of Privacy¹⁷ (the Notice Statement), available online, which states that it collects personal information of students under the authority of the *McMaster University Act, 1976*, in accordance with section 39(2)(a).

[69] The Notice Statement sets out a number of uses for this information, including use for academic and administrative purposes. It directs those with questions regarding collection and use of personal information to the University Registrar or University Secretary. In addition to the Notice Statement, the university has furnished other online

¹⁷ https://pgme.mcmaster.ca/app/uploads/2023/02/FIPPA_Statement.pdf

resources that provide information about Respondus, including “An Introduction to Respondus”¹⁸ and “FAQs on Respondus Online Proctoring” aimed at students.¹⁹

[70] Through these various documents, the university provides students with useful information about Respondus. However, as it now stands, students must search for and consult a number of disparate web pages to discover all the relevant information. Given the sensitivity of the information collected, I find that the spirit and intent of the notice requirement set out in 39(2)(b) of the *Act* is not satisfied by requiring students to consult multiple sources to see the totality of purposes for which their personal information is to be used. I recommend therefore that the university consolidate its notice of collection of personal information via Respondus Monitor in a clear and comprehensive statement, either in a single source document, or with clear cross-references to other related documents, so that students can access this information in a coherent, plain language and accessible way, without having to navigate through a number of other online sources.

[71] The final requirement under section 39(2)(c) is the need to provide the title, business address, and business telephone number of officials to whom questions regarding collection may be directed. Earlier during this investigation, the university stated that the University Registrar or University Secretary could be contacted about general privacy concerns but did not provide a business telephone number for those individuals in compliance with section 39(2)(c). In response to my office’s concerns about this, the university has since addressed the issue by including the name, title, email, and business telephone number of the designated contact person(s) in its online collection notice, satisfying the requirement of section 39(2)(c).²⁰

Issue 4: Was the use of personal information in accordance with section 41(1) of the *Act*?

[72] Section 41(1) of the *Act* limits the use of personal information as follows (in part):

(1) An institution shall not use personal information in its custody or under its control except,

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

(b) for the purpose for which it was obtained or compiled or for a consistent purpose; ...

[73] A “consistent purpose” is explained in section 43 as follows:

¹⁸ https://mi.mcmaster.ca/app/uploads/2021/03/An-Introduction-to-Respondus-_updated.pdf

¹⁹ <https://studentsuccess.mcmaster.ca/respondus-online-proctoring/>

²⁰ The university’s revised collection notice is now titled “Notice of Collection, Use and Disclosure Statement” and is available at <https://secretariat.mcmaster.ca/privacy/notice-of-collection-use-and-disclosure/>

Where personal information has been collected directly from the individual to whom the information relates, the purpose of a use or disclosure of that information is a consistent purpose under clauses 41 (1) (b) and 42 (1) (c) only if the individual might reasonably have expected such a use or disclosure.

[74] Due to the nature of its function, Respondus Lockdown Browser captures limited personal information necessary for the purpose of exam administration. I have already determined that the collection of personal information via Respondus Lockdown Browser for that purpose is authorized under the *Act*. I find therefore that the use of that information for the same purpose is also authorized pursuant to section 41(1) of the *Act*.

[75] In contrast, Respondus Monitor captures much more personal information. It analyzes audio and video footage of a student, using their biometric data and other inputs to assess whether a student's exam session should be flagged to the instructor as a possible academic integrity issue. This personal information is compared with baseline data for all videos analyzed by Respondus Monitor, and with data from other test takers of the same exam. Respondus then weighs the various elements and provides other adjustments before communicating the review priority of the exam session to the instructor.

[76] As I have found, Respondus Monitor collects students' personal information on behalf of the university for its lawfully authorized purpose of proctoring examinations. I also find that it uses the personal information for that same purpose. However, I must go on to consider whether the personal information collected by Respondus Monitor is being used for any other purposes.

[77] From the information provided, it is clear that Respondus uses at least some data gathered from test takers to improve its own services.

[78] In its online information about its products, Respondus describes its own use of student information as follows:

Respondus personnel do not review/analyze the recordings except as may be required to resolve technical problems, improve system performance, modify Respondus Monitor, investigate violations of these Terms, or as may be directed by your Institution or applicable law enforcement.²¹

[79] The Respondus Monitor Terms of Use provides further details on the type of information it may use to improve its system, and how it does so:

²¹ <https://web.respondus.com/privacy/privacy-additional-monitor/>

Random samples of video and/or audio recordings may be collected via Respondus Monitor and used by Respondus to improve the Respondus Monitor capabilities for institutions and students. The recordings may be shared with researchers under contract with Respondus to assist in such research. The researchers are consultants or contractors to Respondus and are under written obligation to maintain the video and/or audio recordings in confidence and under terms at least as strict as these Terms. The written agreements with the researchers also expressly limit their access and use of the data to work being done for Respondus and the researchers do not have the right to use the data for any other purposes. No personally identifiable information for students is provided with the video and/or audio recordings to researchers, such as the student's name, course name, institution, grades, or student identification photos submitted as part of the Respondus Monitor exam session.²²

[80] Respondus states that the random samples of recordings, either audio or video, are not associated with any other direct identifiers that would lead to the student being identifiable. McMaster also describes this as a use of anonymized data, rather than personal information, stating that:

Respondus does collect anonymized, aggregated data on the use of its service to help improve performance, diagnose problems, and detect and prevent fraud and abuse of its services and systems.²³

[81] However, McMaster has already agreed, and I have found, that the video recordings of students are personal information. Further, this office has also previously determined that recordings of an individual contain their personal information.²⁴

[82] Use of personal information for improvement of Respondus' services is clearly not the same purpose for which it was collected, namely to proctor examinations on behalf of the university, nor do I find that it is a consistent purpose. Section 43 of the *Act* stipulates that use of personal information may only be considered to be consistent with the purpose for which it was collected if "the individual might reasonably have expected such a use."

[83] In my view, students would reasonably expect that their university would follow best practices when dealing with their personal information, limit the use of their personal information to that which is necessary to conduct exams with integrity, and not allow third party vendors to use their personal information for purposes unrelated to their education without their consent.

²² <https://web.respondus.com/tou-monitor-student/>

²³ <https://studentsuccess.mcmaster.ca/respondus-online-proctoring/>

²⁴ See Privacy Complaint Report MC07-68, among others.

[84] Students would not reasonably expect that the university, having collected their personal information via Respondus to proctor exams, would permit Respondus to then use that personal information to advance the company's own commercial purposes.

[85] A review of the relevant documents did not identify any ability for students using Respondus Monitor either to consent to, or opt out of, having their video or audio recordings used by Respondus for improvement of its system performance or capabilities.

[86] I find therefore that the use of student audio and video recordings for the purpose of improving Respondus Monitor's system performance or capabilities is not authorized under section 41(1) of the *Act*.

[87] From publicly available information about its services, it appears that Respondus is able to provide Respondus Monitor exam proctoring services without using the personal information in the student recordings for the purposes of improving its services.

[88] Respondus has stated publicly that in some jurisdictions, it does not use personal information to improve its product. In "Algorithmic Fairness and Respondus Monitor Proctoring: A study using Casual Conversations,"²⁵ authored by Respondus' CEO and its Chief Scientist, they note that "[no] data from the European Union, California, and certain other regions are used for research or product improvement purposes." This is consistent with information available on the Respondus' website, which includes separate sections for the privacy protections provided to residents of the EU and California.

[89] Given this apparent ability, I recommend that McMaster secure the written undertaking from Respondus that it will respect Ontario law by ceasing to use students' personal information for system improvement purposes without the consent of students. If such an undertaking is not promptly provided and acted upon, I recommend that McMaster cease the use of Respondus Monitor until such time as it enters into a new particularized agreement with Respondus containing these restrictions, as well as the other provisions recommended below.

Issue 5: Does the university have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students, in accordance with the requirements set out in section 4(1) of Ontario Regulation 460 and sections 4(1) and 5 of Ontario Regulation 459, made pursuant to the *Act*?

[90] When an institution contracts with a third party to provide information management functions, the institution's obligations to comply with *FIPPA* continue. As such, there must be contractual and oversight measures in place to ensure that the institution remains in compliance with the *Act*.²⁶

²⁵ Available at https://web.respondus.com/wp-content/uploads/2022/04/Algorithm_Fairness_4.7.22.pdf

²⁶ Ontario Criminal Code Review Board [1999] O.J. No. 4072 (C.A.) and Privacy Complaint Report PR16-40.

[91] McMaster has contracted with Respondus to provide exam proctoring services. Under the *Act*, the university remains responsible for the security, retention and destruction of personal information in its custody or control.

[92] Ontario Regulation 460, made pursuant to the *Act*, establishes rules for the security and retention of records in the custody of an institution. Section 4(1) of that regulation requires that institutions define, document, and put in place measures that are reasonable to prevent unauthorized access to the records in their custody or control, including records containing personal information. Ontario Regulation 459 under the *Act* sets out specific rules governing the secure disposal and destruction of personal information.

[93] Each institution is different and may devise its own approach to meeting the requirements in Regulation 460. As noted by Investigator Lucy Costa in Privacy Complaint Report PR16-40, the regulation does not prescribe a “one-size-fits-all” approach to security:

It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have “reasonable” measures and ties those measures to the “nature” of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.²⁷

[94] Where an institution subject to the *Act* retains a private sector entity to provide core functions on its behalf, it must take all reasonable and appropriate measures to ensure that the entity deals with the records under the control of the institution in ways that comply with the institution’s obligations under the *Act*. The principal means by which the institution may achieve this objective is through provisions in its contract with the private sector entity that ensure the services performed on the institution’s behalf comply with the rules and safeguards set out in the *Act*.²⁸

Contractual and Business Relationship

[95] Respondus and McMaster signed a “LockDown Browser License Agreement for Non-Profit Educational Institutions” (License Agreement) for the 2020-21 school year, which has since been renewed. The License Agreement is largely focussed on the rights conferred on McMaster to use Respondus’ software, and the monetary cost associated

²⁷ Privacy Complaint PR16-40 at para 72.

²⁸ Ibid. at paras 116-117.

with this. The License Agreement lists the "Software Product" as LockDown Browser, and refers to Respondus Monitor as an "optional, companion service" that the Licensee "can enable or disable ... during the License Term, subject to a separate Terms of Use agreement." The annual fees listed in the License Agreement include amounts specific to both LockDown Browser and Monitor, with Monitor usage forming the bulk of the associated cost.

[96] McMaster did not provide any separate agreement or contract specific to Respondus Monitor. However, it appears that Respondus has general terms in place for institutions that do not enter into a particularized agreement with Respondus regarding the use of Monitor.

[97] On its website, Respondus publishes a document titled "Terms of Use – Respondus Monitor (Institution)" (Monitor TOU)²⁹. The preamble to this document states that it is provided for reference, that terms may vary by region, and "[c]ertain institutions may also use customized versions of these terms." The Monitor TOU states that it is an agreement between the institution and Respondus "regarding the Institution's use of Respondus Monitor," specifying that the institution "agrees to these Terms in full before using Respondus Monitor."

[98] McMaster has been using and paying for the use of Respondus Monitor since 2020. According to the Monitor TOU, once it started using this service, the Monitor TOU came into effect. Given this, and in the absence of a separate agreement between Respondus and McMaster regarding Respondus Monitor, the provisions in the Monitor TOU apply between McMaster and Respondus.

[99] Respondus also publishes the following privacy-specific information regarding its products:

- Data Processing Agreement³⁰
- Respondus Product Privacy Policy (Privacy Policy)
- Additional Privacy Information – Respondus Monitor (Monitor Privacy Information)
- Additional Privacy Information – LockDown Browser (LockDown Privacy Information)

[100] The License Agreement does not substantively address privacy or security matters but is specifically linked to the Privacy Policy. Further, the Data Processing Agreement states in its preamble that it forms part of the License Agreement. The Monitor TOU states

²⁹ <https://web.respondus.com/tou-monitor-admin/>

³⁰ <https://web.respondus.com/data-processing/>.

that it incorporates by reference both the Privacy Policy and the Data Processing Agreement. There is no mention of the Monitor Privacy Information or the LockDown Privacy Information being incorporated by reference or otherwise forming part of the contractual agreement.

[101] In Privacy Complaint Report PR16-40, Investigator Costa enumerated the contractual provisions that may be relevant in assessing whether the institution in that matter had discharged its obligations to ensure that all reasonable steps were taken to protect the privacy and security of personal information under its control. These included provisions relating to:

- Ownership of Data
- Confidential Information
- Collection, Use and Disclosure
- Notice of Compelled Disclosure
- Subcontracting
- Security
- Audits
- Retention and Destruction

[102] I adopt this assessment framework and address below the adequacy of McMaster's contractual and oversight measures governing its relationship with Respondus.

Ownership

[103] The Data Processing Agreement describes Respondus as a "processor" of personal information, stating that the licensing institution "maintains ownership and controls all access to the Licensee data in its account." The Data Processing Agreement also states that Respondus will not access any Licensee Data except as necessary for the operation of the services or as expressly permitted by the Licensee, unless otherwise required by law to do so.

[106] In addition, the Monitor TOU states that "Respondus does not claim ownership in the information or data [the institution] or any students provide". The Monitor TOU goes on to state that Respondus has a license to "use, store, modify, copy, and transmit any such information or data" but limits the purposes of doing so to the carrying out of services in accordance with the Monitor TOU.

[104] Based on the above, I am satisfied that McMaster retains ownership of the information held by Respondus.

Confidential Information

[105] Respondus uses the term “personal data” which it defines in the Data Processing Agreement as having the meaning set out in the applicable data protection law. “Personal data” under the Data Processing Agreement therefore incorporates the definition of “personal information” found in s. 2 of the *Act*.

[106] The Privacy Policy, incorporated by reference into the Monitor TOU, also provides the following definition:

Personal data is a name, address, telephone number, email address, identification number, online identifier, or other data collected that could directly or indirectly identify you. This is also known as Personal Information or Personally Identifiable Information (PII).

[107] The Privacy Policy describes Respondus’ use of personal data generally as follows:

We strongly believe in both minimizing the personal data we collect and limiting its use and purpose to only: (1) that for which we have been given permission, (2) that which is necessary to deliver the products you purchase or interact with, or (3) as we might be required or permitted for legal compliance or other lawful purposes.

[108] The Privacy Policy differentiates between aggregate data and information that is either personal data or may be linked to personal data, as follows:

Much of the data collected is aggregated or statistical data about how individuals use our Services, but to the extent that product data is itself personal data, or is linked or linkable to personal data, we treat it accordingly.

[109] The Data Processing Agreement states that Respondus may “de-identify Licensee Data ... and may process De-Identified Data to maintain and improve the services.”

[110] Taken together, the provisions in the Data Processing Agreement and the Monitor TOU (including the incorporated Privacy Policy) do not provide adequate protections for the personal information contained in video and audio recordings.

[111] Respondus uses samples of video and audio recordings to improve its services, stating that these samples do not have any *other* identifying information associated with them³¹ and appears to treat them as de-identified data. However, I have already found that video and audio recordings of individual students can be used to identify the student

³¹ See “Privacy and Security Policy” section of Monitor TOU, available at <https://web.respondus.com/tou-monitor-admin/>

and that such recordings constitute the student's personal information whether or not they are associated with other identifiers.

[112] Given this, I am not satisfied that Respondus affords to these sample recordings the same confidentiality protections afforded to other personal information. I recommend therefore that McMaster seek confirmation from Respondus that it will treat and protect all audio and video recordings, regardless of length, and any inferences or information related thereto, as personal data.

Collection, Use, and Disclosure

[113] The Monitor Privacy Information states that during exams, Respondus creates a facial template to determine if the student who started the exam differs from the person in the video frame throughout the duration of the exam.³² It also states that the template is not saved on the student's computer or to the cloud server database, and it is cleared from the computer immediately after exam completion, and from the server's memory no later than two days after exam completion. It appears from the foregoing that Respondus has undertaken to collect no more facial detection information than is necessary for functional purposes, that its use is limited to those purposes, and that the facial data collected is deleted after a reasonably short period of time.

[114] As outlined above, the Data Processing Agreement limits Respondus' access to the Licensee Data to what is necessary for the operation of the services, expressly permitted by the Licensee, or required by law. The Privacy Policy outlines similar restrictions and states that Respondus minimizes the personal data it collects.

[115] As noted above, however, Respondus appears to regard the video and audio recordings as de-identified data that may be used to maintain or improve its services and system performance. This is confirmed by the Monitor TOU which states that Respondus uses video and/or audio recordings to improve Respondus Monitor's capabilities, and that this may include sharing these recordings with researchers under contract with Respondus without providing them with any personally identifying information.

[116] For the reasons outlined above, I am not satisfied that the Data Processing Agreement, Monitor TOU, and Privacy Policy provide adequate protection for the collection, use, and disclosure of the personal information in the video and audio recordings. To address this, I reiterate my recommendation that McMaster secure a written undertaking from Respondus that it will cease the use of students' personal information for research or product improvement purposes without the consent of students.

³² <https://web.respondus.com/privacy/privacy-additional-monitor/>

Notice of Compelled Disclosure

[117] The Privacy Policy addresses the circumstances in which Respondus may disclose personal information to authorities, stating:

Respondus does not voluntarily or actively transfer or disclose our customers' personal data to government or law enforcement authorities. In the event of a request from a government or law enforcement authority, we have procedures and controls in place to make sure that such a request is assessed and challenged to confirm its validity.

[118] The Monitor TOU states that Respondus "reserves the right at all times to disclose any information or data (including recordings and any content to the extent applicable) ... to comply with the law."

[119] After reviewing the relevant documents, I was not able to find any requirement that Respondus notify the Licensee in the event that it is required to disclose a user's personal data to authorities. An institution should require service providers to provide it with prompt notice of any such compelled disclosure of personal information to government or law enforcement to allow it to seek an appropriate remedy to prevent or limit such disclosure. Further, the institution should require the service provider to disclose only the personal information it is legally compelled to disclose. Accordingly, I recommend that McMaster should secure a written undertaking from Respondus incorporating the above-noted requirements.

Subcontracting

[120] The Data Processing Agreement states that any person authorized to process Licensee Data, including subcontractors, shall be subject to a "legally-binding duty of confidentiality" and that Respondus shall ensure that authorized persons, including subcontractors, shall maintain the security of this data and process it only as necessary for operation of the services or as expressly permitted by the Licensee.

[121] The Data Processing Agreement permits subprocessing, as Respondus' servers are operated by a third-party hosting provider, that is a subprocessor under applicable data protection law. This agreement states that the Licensee consents to the appointment of this subprocessor but notes that "Respondus shall impose data protection terms that are consistent with the terms of this DPA and the Applicable Data Protection Laws." The Data Processing Agreement further specifies that "Respondus remains fully liable for any breach of this DPA by any act, error or omission of its Subprocessor."

[122] However, as noted above, the Monitor TOU also contemplate subcontracting research on the use of sample recordings to maintain or improve Respondus Monitor services. I have already determined that this does not provide adequate protection of

students' personal information. I reiterate my recommendation that McMaster seek an express undertaking or include provisions in a particularized Respondus Monitor Terms of Use Agreement prohibiting the use or disclosure of personal information, including video or audio recordings, for the purpose of improving Respondus' system or similar purposes.

Security

[123] The Data Processing Agreement addresses security measures as follows:

Respondus shall implement appropriate technical and organizational measures to protect the Licensee Data from unlawful processing and/or a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the nature, likelihood and severity of the risk to the rights and freedoms of natural persons.

[124] The Data Processing Agreement goes on to set out the measures it shall take, as appropriate, as part of the security protections, including the encryption of personal data, the ability to restore and access personal data in a timely manner if an incident occurs, and a process for regularly testing and evaluating the effectiveness of the measures in place.

[125] The Respondus Data Processing Agreement also requires Respondus to notify Licensees in the event of a breach, stating as follows:

If Respondus becomes aware of an actual Security Incident³³ that involves Licensee Data, Respondus will: (a) notify Licensee of the Security Incident without undue delay; (b) take appropriate steps to identify the cause of the Security Incident, minimize harm and secure the Licensee Data; and (c) provide Licensee with information as may be reasonably necessary to assist Licensee with its notification and reporting responsibilities.

Audits

[126] The Data Processing Agreement provides Licensees with the right, once a year, to submit audit questions relating to Respondus' processing and protection of data. Respondus is required to respond to those questions. It is also required to "maintain complete and accurate records and information to demonstrate its compliance with [the Data Processing Agreement]" and make these records available for audit by its Licensees.

³³ The Data Processing Agreement defines "security incident" as a personal data breach under the European Union's General Data Protection Regulation.

Retention and Destruction

[127] The Data Processing Agreement states that Respondus will retain Licensee Data for the period of time described in the License Agreement and Monitor TOU and elaborates on the deletion of data as follows:

Upon termination of the Licensee's elected data retention period, or upon request of the Licensee, Respondus shall delete all Personal Data processed on behalf of the Licensee, unless a further period of time is provided for the storage of Personal Data under a provision of Applicable Data Protection Law. Upon request, Respondus shall provide a written statement confirming the deletion of the Licensee Data along with the deletion of all existing copies of the Licensee Data, within and no later than 7 (seven) days from the deletion of the Licensee Data.

[128] In addition to the overall retention policy described in the Data Processing Agreement, the Monitor Privacy Information states that the "temporary template of facial identifiers" used during an exam session is not saved to the cloud server's database or storage and is cleared from the server's memory no later than two days after the exam is completed.

[129] As for the audio and video recordings captured through Respondus Monitor, these are created during exams for the purposes of ensuring that students are not cheating in that course. Therefore, any possible utility of the recordings would reasonably end with the conclusion of the course term. I recognize that McMaster operates several different academic terms, and that some courses are multi-term courses. Given this, I recommend that McMaster contractually require Respondus to delete McMaster's data from its servers on, at minimum, an annual basis, unless McMaster requests otherwise, and that Respondus provide confirmation of this deletion.

[130] In specific cases that lead to academic integrity investigations requiring the review of audio and video recordings captured through Respondus Monitor, the university states that such recordings would be subject to the records retention policy for academic integrity investigations.

[131] In respect of Respondus Lockdown Browser, McMaster stated in its PIA Summary that students could remove the software after the exam has concluded and it is no longer necessary. McMaster acknowledged to my office that it had not looked into whether this removal entirely wiped the Respondus software from student computers. I recommend that McMaster conduct tests to confirm that uninstalling Respondus after an exam actually results in the removal of the totality of that software, with no remnants of it remaining on the computer.

Other Recommendations

[132] McMaster has adopted a tool that employs artificial intelligence technology to automate proctoring exams online and help inform inferences or decisions about academic integrity that can have significant impacts on its students.

[133] My analysis and recommendations above pertain to McMaster's current statutory obligations to protect students' personal information under the *Act*. Although there is no current law or binding policy specifically governing the use of artificial intelligence in Ontario's public sector, I recommend that McMaster build in additional guardrails to protect its students from the heightened risks associated with its AI-enabled proctoring software.

[134] Together with my counterparts across Canada³⁴ I have called for strong guardrails to ensure AI systems, including generative AI, are safe, privacy protective, transparent, accountable, and human rights affirming.

[135] The Government of Ontario has acknowledged the need to develop guardrails for the use of artificial intelligence technology in the public sector and is in the process of developing Ontario's Trustworthy Artificial Intelligence (AI) Framework.³⁵

[136] In a joint statement I issued with the Chief Commissioner of the Ontario Human Rights Commission³⁶, we urged the government to press forward with finalizing its Trustworthy AI framework into a binding set of robust and granular rules that effectively address safety, privacy, accountability, transparency, and human rights. We set out our rationale in the Joint Statement as follows:

AI technologies have great potential to benefit society in terms of improved health, education, public safety, and social and economic prosperity. However, they have also been shown to be unsafe when not effectively governed. They often rely on immense volumes of personal information, which may not be properly protected, and the initial collection of this information may not always be lawful. Even where information has been de-identified, AI technologies can perpetuate biases and lead to disparate impacts on Ontarians. This is particularly true for historically marginalized individuals or groups, including those protected under human rights legislation.

³⁴ Principles for responsible, trustworthy and privacy-protective generative AI technologies, December 7, 2023, https://priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/

³⁵ <https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework>

³⁶ Joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies, May 25, 2023, online: https://www.ipc.on.ca/?post_type=news-release&p=21033

AI technologies can support the drawing of inferences and decision-making processes that are opaque or difficult to understand or challenge. The use of AI technologies, especially generative AI systems, may create flawed or inaccurate content that raises concerns about how government can ensure accountability for their use. All of those risks are compounded where AI technologies are not adequately evaluated before and after their adoption, including the risks of ingraining or amplifying historical systemic biases or discriminatory practices. The harms presented by those risks can be more damaging without meaningful engagement with potentially affected parties about whether to develop, acquire, or deploy these technologies, including what rules should govern their use.

[137] I acknowledge that the university has already carried out a level of due diligence prior to adopting Respondus Monitor, including carrying out a pilot project, completing a PIA, examining the vendor's policies, protocols and terms of use, and developing its own policies and related communication materials, such as FAQs for both teachers and students on how the AI software works. However, given the significant risks and potential harms associated with AI tools that can adversely impact students' rights, I recommend that McMaster go further by adopting additional guardrails, including the following.

PIA and Algorithmic impact assessment

[138] Given the broad range of privacy and human rights and impacts at stake with AI, I recommend that McMaster undertake an algorithmic impact assessment (AIA)³⁷ in addition to its PIA. An AIA is an additional tool that contains a series of questions and prompts to help organizations assess the potential impacts of an automated decision-system.

[139] An AIA will help assess the level of risks associated with the university's use of Respondus Monitor for the purpose of proctoring online exams, conduct a higher level of scrutiny over the source or provenance of the data used to train its algorithms, and consider the potential impacts it can have not only on the rights of individual students, but on the interests of broader communities of students on campus and the overall level of public trust in the university. Most importantly an AIA can help the university identify and focus on concrete ways of mitigating some of these risks and potential impacts.

[140] In its response to an earlier version of this report, the university has committed to using the Treasury Board of Canada's tool to conduct AIAs as part of its privacy impact assessments. This is particularly important until such time as Ontario develops a similar tool for its public and broader public sectors.

³⁷ For example, see Treasury Board of Canada's Algorithmic Impact Assessment tool available at: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>

Consultation with affected communities

[141] Ideally, institutions considering adopting AI technologies should meaningfully engage and consult with affected parties and those with relevant expertise prior to adoption, and on a regular basis thereafter. This consultation is critical for understanding the full scope of potential issues that may arise, and how these issues may impact, be perceived, and be experienced by others.

[142] Being attentive to these considerations from the start and throughout implementation allows the institution to be alert to issues that may arise, respond quickly to change its approach mid-course, and if need be, reassess whether to proceed with using the technology, or move towards a different approach less prone to such pitfalls.

[143] I recommend that McMaster carry out this necessary consultation step with representatives of its many diverse communities among its student population, particularly those from vulnerable or historically marginalized groups. These consultations should also include necessary experts in privacy and human rights, as well as technologists with relevant expertise to understand how the underlying algorithms work and their potential adverse or differential impacts on communities.

Broader opportunity for students to opt-out

[144] It is a known fact that AI technologies are not necessarily neutral or accurate. Bias within an algorithm may have the unintended effect of reinforcing discrimination towards vulnerable and historically marginalized communities or arriving at decisions that are individually or systematically unfair or unjust.

[145] For example, the video component of automated exam proctoring may result in certain individuals or groups being treated differently. Some research suggests that individuals with darker skin tones are flagged more often.³⁸ Others have noted that the students with certain disabilities may involuntarily move or speak in a way that would also lead to additional flagging and potentially false positives.³⁹

[146] In McMaster's case, students with disabilities are accommodated by using live invigilation, rather than automated proctoring through Respondus Monitor. However, AI-powered technologies may potentially trigger other protected grounds under human rights that require similar accommodations, such as color, race or ethnic origin.

³⁸ Racial, skin tone, and sex disparities in automated proctoring software, *Frontiers in Education*, September 2022, available at <https://doi.org/10.3389/feduc.2022.881449>. Respondus' own publication, "Algorithm Fairness and Respondus Monitor Proctoring: A study using Casual Conversations" also found an increased error rate in poor lighting conditions for the darkest skin tone classification.

³⁹ How Automated Test Proctoring Software Discriminates Against Disabled Students, Lydia X. Z. Brown, November 16, 2020, available at <https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/>

[147] It is not within my mandate to make findings or recommendations under human rights law. However, I encourage McMaster to make special arrangements not only for students requesting formal accommodation under a protected ground in human rights legislation, but also for any other students having serious apprehensions about the AI-enabled software and the significant impacts it can have on them and their personal information. Now that in-person invigilation is possible post COVID, all students should be provided with the general opportunity to opt out of online exam proctoring in favor of in-person exams depending on their personal circumstances and general level of comfort with this relatively invasive technology.

Human Supervision and ability to challenge results

[148] Institutions remain ultimately responsible for ensuring the accuracy of the data they use and the validity of decisions they make based on information the AI tool provides, infers or generates.

[149] McMaster has built in an appropriate level of human oversight over Respondus Monitor by ensuring that any flags detected by the software are brought to the attention of the instructor. The instructor is to review the flag and begin a conversation with the student if there is a concern. The instructor can only review the video upon request and as appropriate, and only then can a charge be brought under the Academic Integrity Policy and a potential investigation into potential academic misconduct ensue.

[150] In its student FAQs on Respondus Online Proctoring, under the section entitled "What if...?", McMaster tells its students "not to worry" and "don't panic" if the system happens to flag their movements or their conduct as suspicious, explaining that their instructor will conduct a review of the recording. "This means it will be up to a human, and not a computer, which cases are investigated further."

[151] The FAQs go on to describe possible scenarios that might occur, and suggest how students may try to avoid them, or if they do happen, how students can explain them during the exam, or immediately thereafter, and to whom.

[152] The FAQs later explain that the audio and video recordings taken of students, as well as any additional information about the student's computer use during the exam, will be assessed by the instructor to determine whether a flagged case requires further follow up, including referral as a possible breach of McMaster's Academic Integrity Policy.

[153] However, the FAQs are silent in terms of explaining how students can challenge allegations or inferences made about them by the instructor, based on flags identified by the proctoring software. Presumably, at that point, the full weight of the university's academic integrity policy comes to bear on the rights and obligations of the parties, including the student's right to a hearing.

[154] However, given the fallibility of many AI tools, I recommend that McMaster provide a less formal means for students to challenge flags identified by the Respondus Monitor software, including their instructor's subsequent review, prior to invoking the formal academic integrity process that can be a very heavy one. Students should be provided with a meaningful opportunity to explain their situation. Where warranted, students should have the right to correct the information, and have the flag removed and any inferences or allegations based on the flag deleted from their student record. It is possible that McMaster already provides students with this informal opportunity to explain in practice. However, I recommend that its FAQs aimed at students provide explicitly for the possibility of this informal step and communicate it in a way that is understandable and actionable for its intended audience.

Use of vendors

[155] Institutions choosing to use AI technologies must remember that these tools are working for them, and pursuant to their statutory authorities and obligations. While they can outsource their data processing functions, they cannot outsource their responsibility. Ultimately, the institution should not satisfy itself with AI technology that operates in a "black box", without being able to understand and explain how the technology functions.

[156] Organizations should ensure that the vendor of any AI tool selected has designed its tool in a manner that ensures safe and accurate results, accounts for heightened privacy and security concerns which may be associated with AI technology, and mitigates against any potential bias and discriminatory impacts.

[157] In its online FAQs, McMaster assures its students that it has conducted an in-depth review of Respondus' data security and privacy practices in the context of its PIA. This includes having reviewed the company's publicly available material such as its privacy policy and terms of use, as well as its internal policies and protocols for greater detail on its collection, use, access and disclosure of personal information, and its security safeguards and incident management protocols.

[158] However, it is not clear whether McMaster has enquired into other aspects of Respondus Monitoring software, such as how the algorithm works and the provenance of the data used to train the system.

[159] As a private sector organization, Respondus falls outside my office's jurisdiction and a full review of the company's operations is beyond the scope of my mandate.

[160] However, as explained above, McMaster remains accountable for the protection of its students' privacy rights and any decisions it makes based on the personal data it collects about them, even when it outsources data processing capabilities, including AI, to third party vendors.

[161] The use of AI technologies in exam proctoring is not particular to Respondus, as there are other competitors who provide similar services⁴⁰. However, if McMaster is contemplating continuing its business relationship with Respondus and decides to enter into a particularized agreement in respect of the Respondus Monitor software, the university should conduct greater scrutiny over how this tool was developed and how it is used.

[162] Specifically, this means that in addition to the provisions I recommend McMaster include in its agreement with Respondus outlined above, I recommend that the university also ensure that any data used by Respondus to train its algorithms was obtained in compliance with Canadian laws, and in keeping with Ontarians' reasonable expectations of privacy.

[163] Furthermore, I recommend that in its negotiation for a particularized agreement for the use of Respondus Monitor, McMaster should prohibit the use of its students' personal information for algorithmic training purposes, unless the company can demonstrate a process for obtaining their meaningful consent.

[164] On a broader level, McMaster remains accountable for the continued use of AI technologies throughout their lifecycle and across the variety of circumstances in which they are used. This includes continually evaluating the reliability of the tool. Even once a particularized agreement is in place for the use of Respondus Monitor, McMaster should continue to monitor for and alert Respondus to potential inappropriate uses or biased outcomes that may not have been disclosed as a potential limitation of their system. Conversely, McMaster should require Respondus to also monitor for, and inform the university of any weaknesses, biases or vulnerabilities it discovers about the program.

[165] The adoption and application of the above guardrails would allow institutions such as McMaster to make responsible use of AI technologies to help carry out its lawfully authorized activities, while protecting against discriminatory impacts and promoting students' privacy. I acknowledge that several of McMaster's practices already demonstrate an understanding of the heightened need to protect the privacy rights of students when utilizing these types of technologies. However, to the extent there may be gaps, I recommend McMaster adopt the additional guardrails above and build them into its online proctoring program and/or its contractual provisions with Respondus as appropriate.

⁴⁰ See, for example, "Examity Launches AI Enabled Proctoring Solution at UC Davis" available at <https://www.examity.com/examity-launches-ai-enabled-proctoring-solution-at-uc-davis/> and "Paving the Way for Ethical Technology" available at <https://proctorio.com/about/blog/paving-the-way-for-ethical-technology>.

CONCLUSION:

1. The students' names, course information, biometric data, photo identification, and audio and video recordings are "personal information" as defined in section 2(1) of the *Act*.
2. The collection of personal information via Respondus LockDown Browser and Respondus Monitor is in compliance with section 38 of the *Act*.
3. The university's notice of collection does not comply with 39(2) of the *Act*.
4. The use of personal information via Respondus LockDown Browser on behalf of the university is authorized under section 41(1) of the *Act*, but the use of personal information via Respondus Monitor for product improvement purposes is not in compliance with section 41(1) of the *Act*.
5. The contractual and oversight measures in place are not sufficient to ensure the privacy and security of the personal information of its students, in accordance with the requirements of section 4(1) of Ontario Regulation 460 and sections 4(1) and 5 of Ontario Regulation 459 made pursuant to the *Act*.

RECOMMENDATIONS:

1. The university should consolidate its notice of collection of personal information via Respondus Monitor in a clear and comprehensive statement, either in a single source document, or with clear cross-references to other related documents, so that students can access this information in a coherent, plain language and accessible way, without having to navigate through a number of other online sources.
2. The university should secure a written undertaking from Respondus that it will cease using students' personal information for service improvement purposes and disclosing students' personal information to subcontractors for research purposes, without the consent of students. If Respondus does not promptly provide and act upon such an undertaking, I recommend that McMaster cease the use of Respondus Monitor until such time as it enters into a particularized

agreement with Respondus containing these and other restrictions, recommended below.

3. The university should seek confirmation from Respondus that it will treat and protect all audio and video recordings, regardless of length, and any inferences or information related thereto, as personal data.
4. The university should secure a written undertaking from Respondus that in cases of compelled disclosure of personal information to government or law enforcement, it will provide McMaster with prompt notice of any such compelled disclosure to allow it to seek an appropriate remedy to prevent or limit such disclosure. Further, the written undertaking should require Respondus to disclose only the personal information it is legally compelled to disclose.
5. The university should contractually require that Respondus delete personal data from its servers on an annual basis, minimally, and that it provide the university with confirmation of data deletion when it occurs.
6. The university should conduct tests to confirm that uninstalling Respondus LockDown Browser actually results in the removal of the totality of that software, with no remnants of it remaining on the computer.
7. The university should adopt additional guardrails for the heightened privacy risks associated with the use of its AI-enabled exam proctoring software in its program and policies, and in its contractual relationship with Respondus where appropriate. These include guardrails to:
 - a. conduct an algorithmic impact assessment, in addition to a PIA;
 - b. carry out consultation with representatives of its many diverse communities among its student population, particularly those from vulnerable or historically marginalized groups;
 - c. provide students with an opportunity to opt out of online proctoring, and choose in person invigilation instead;

- d. provide a less formal means for students to challenge flags identified by the Respondus Monitoring software prior to invoking the formal academic integrity process, and inform students more explicitly of this possibility;
- e. Conduct greater scrutiny over how the Respondus Monitoring software was developed to ensure that any source data used to train its algorithms was obtained in compliance with Canadian laws and in keeping with Ontarians' reasonable expectations;
- f. Prohibit Respondus from using students' personal information for algorithmic training purposes without their consent; and,
- g. Continue to monitor for, and document, any inappropriate uses or biased outcomes that may not have been disclosed as a potential risk of limitation of the software and inform the vendor accordingly, and require Respondus to do and inform it of same.

Within six months of receiving this Report, the university should report back to my office regarding the implementation of these recommendations.

Original signed by: _____

Patricia Kosseim
Commissioner

February 28, 2024

Appendix G

Considerations for privacy and confidentiality in adolescent health care service delivery



Principal author(s)

Holly Agostino MD, Alene Toulany MD; Canadian Paediatric Society, Adolescent Health Committee, Adolescent Health Committee

Paediatr Child Health 2023 28(3):172–177. (<https://academic.oup.com/pch/article-pdf/28/3/172/50336728/pxac117.pdf>) 

Abstract

A hallmark of delivering quality adolescent health care services is the provision of confidential care. Key tenets when providing confidential care for adolescents include time alone with a health care provider, maintaining privacy of health information, and securing informed consent for services without permission from a parent, guardian, or caregiver. While confidentiality is a basic principle for all health care encounters regardless of age, the unique considerations for capable adolescent patients are not always realized or appreciated. By ensuring appropriate quantity and quality of confidential care for adolescents, clinicians are better equipped to elicit a comprehensive history and physical examination, while empowering the adolescent involved to develop agency, autonomy, trust, and responsibility for their own health care decision-making and management.

Keywords: Adolescent; Confidentiality; Consent; Electronic Health Record; Privacy

The importance of providing confidential care for adolescents cannot be overstated. Confidentiality is defined as an agreement between the patient and health care provider (HCP) that information discussed during medical encounters will not be shared with other parties without the patient's explicit consent ^[1]. A comprehensive history and physical examination that includes sensitive personal information is often required for clinical decision-making involving adolescents. Full and truthful disclosure by individuals is essential to ensuring appropriate diagnostic testing and therapeutic management. Ensuring privacy and maintaining confidentiality are critical for effective, sensitive management of potentially stigmatizing health issues and enhanced quality care ^[2]. Despite clear advantages, the delivery of confidential services remains suboptimal for adolescents in Canada ^[3].

The need for confidential care in all health-related encounters with adolescents has been endorsed by numerous international and national societies ^[4] ^[7]. Studies indicate that adolescents are more likely to access health care and disclose sensitive health information when confidentiality is assured ^[8] ^[9]. Concern regarding privacy is often cited as the primary barrier preventing adolescents from seeking health care services ^[9]. In particular, adolescents are less likely to openly communicate with HCPs around issues related to substance use, mental health, and sexuality when confidentiality cannot be guaranteed ^[10]. Moreover, without confidential care, adolescents may decline routine services, such as sexually transmitted infection (STI) testing, or not engage in follow-up care ^[11].

Ensuring the proper provision of confidential care is also critical to the adolescent developmental trajectory. Time alone with HCPs fosters adolescent independence and the development of skills to better navigate both paediatric and adult health care systems ^[12]. The autonomy and decision-making competencies nurtured by these interactions support age-appropriate developmental milestones essential for successfully transitioning to adult care ^[12].

Legal framework

In Canada, federal legislation such as the Privacy Act and the Personal Information Protection And Electronic Documents Act (PIPEDA) govern the collection, use, and disclosure of personal health information ^[13] ^[14]. These acts specifically recognize the right to privacy of all patients during medical encounters but do not specify the age or circumstances to consider when determining the rights of young people to confidential care. Moreover, each Canadian province and territory has legislation regarding health record privacy protections, some of which takes precedence over PIPEDA. In most provinces and territories, responsibility is placed on the HCP to determine whether a particular adolescent's confidentiality should be maintained based on individual circumstances, with consideration of the patient's psychosocial development and maturity, behaviours, and family-related contextual factors. When an adolescent is deemed a "mature minor" (i.e., is found to have the capacity and maturity to make health care decisions alone) and no risk to self is apparent, they may then consent to having their health records kept private ^[15]. Two provinces diverge from the mature minor doctrine at the present time. In Quebec, the Act Respecting the Health Services and Social Services ^[16] specifically states that adolescents 14 years of age or older have the right to control access to their medical record. Similarly, Newfoundland and Labrador accord the right to privacy of medical information at age 16 ^[17]. In both provinces, parents continue to have access to their adolescent's medical information before the ages specified by law.

Confidentiality versus consent

Confidentiality and consent are closely related but distinct concepts. While confidentiality focuses on keeping health information private, consent laws centre on the determination of decision-making capability. In general, informed consent requires that a decision-maker has the capacity to make a decision, is given all relevant information, and is making a voluntary decision freely, without coercion ^[18]. There is no universally accepted, legally defined age of consent for health care decision-making in Canada. Therefore, just as with right to confidentiality, the capacity of adolescent patients to consent to a proposed treatment varies with age and circumstances and must be determined on a case-by-case basis. Similar to confidentiality laws, Newfoundland and Labrador ^[17] and Quebec ^[19] identify a specific age at which a minor can consent to low-risk treatments. All other provinces or territories in Canada function on the mature minor doctrine.

Limits to confidentiality

Even when the law explicitly protects the confidentiality of health information for adolescents, it may be permissible or even necessary to breach confidentiality in certain circumstances. Both the adolescent and the parent, guardian, or caregiver should be made aware of these circumstances by the HCP involved. Specifically, when an HCP deems that an adolescent is at risk of seriously harming themselves or others, confidentiality must be breached ^[20].

Furthermore, each province or territory has legislation requiring physicians (or other clinicians) to report to protective authorities when an adolescent is in need of protection. The provision includes reporting certain communicable diseases to public health, for example. HCPs may also be required to disclose confidential patient information due to a court order. HCPs must be aware of, and conversant with, the federal and provincial/territorial legislation affecting health care privacy and confidentiality in their jurisdiction.

Family-based considerations for confidential care

Adolescent concerns

While adolescents may have a basic understanding of confidentiality, many are unaware of the specific protections that apply when they receive health services ^[21]. HCPs should routinely counsel the adolescents they see regarding their right to confidential health care, along with any limits that may apply. Education on rights to privacy and confidential health care delivered through school-based or community health promotive programs could further alleviate concerns that might prevent adolescents from seeking health care. While some studies have shown that adolescents value confidentiality when interacting one-on-one with an HCP, others suggest that they can also experience discomfort during such encounters ^[22]. Feelings of uneasiness around discussing sensitive information, and concern about subsequent questions from parents or caregivers have been reported. Clear, routine discussions with adolescents *and* a parent or caregiver about the protections (and limits) of confidentiality before the medical encounter is initiated can help mitigate these concerns.

Beginning in early adolescence, spending at least part of each health visit alone with an adolescent patient, at regular intervals if not for every encounter, conveys the message that this is a routine practice and a valued part of health care. This private time provides opportunities for developing a trusting patient-provider relationship and invites discussion of sensitive health topics in an open and non-judgemental manner. Should a physician feel uncomfortable about being alone with a patient or reviewing certain sensitive topics, it is appropriate to consider a chaperoned discussion with another HCP present ^[23].

Parent or caregiver expectations

Studies suggest that parent and caregiver views on adolescent confidentiality are mixed, with physicians citing fear of parental resistance as a potential barrier to providing confidential care ^[24]. While most parents and caregivers appear to acknowledge and recognize the benefits of adolescent confidentiality ^[25], they also report having concerns that confidentiality may promote risky behaviours or undermine their own protective role ^[22]. Family members or caregivers might also believe that an adolescent feels comfortable discussing sensitive topics in their presence, and they may wish to be present to help intervene if something negative is impacting their adolescent's life.

To alleviate these fears, HCPs should consider communicating with parents early on around the developmental appropriateness—and the laws affecting—confidential health care for adolescents, and its demonstrable benefits. Posting notices in the waiting room to remind patients and families about the importance of confidential care may be beneficial. Also, confidential time should be presented to parents and caregivers as a routine part of the health care visit. HCPs are discouraged from asking in the presence of a parent or caregiver whether an adolescent would like time in private, because the adolescent may feel uncomfortable with, or even reluctant, to agree.

In many circumstances, it is appropriate to encourage and support adolescents in discussing their health issues with a parent or caregiver. The Society for Adolescent Health and Medicine (SAHM) and the American Academy of Pediatrics (AAP) encourage adolescents to discuss health issues with their parents while also supporting their right to privacy^[5]^[26]. This combined approach might involve discussion with adolescents about how they perceive a specific disclosure to parents, helping them to weigh the potential advantages of more open communication, and offering to facilitate communication with parents in ways that help the patient. Remember that some adolescents do not have parental support or, indeed, any meaningful connection with their families. In some cases, the disclosure of sensitive information to a parent or caregiver could put the adolescent at risk (e.g., of abuse, maltreatment, or being ‘kicked out’ at home). When clinicians encourage adolescents to communicate openly with their parents, it is essential to ask first about why they are reluctant to do so.

Health system considerations

Technology

A fast-evolving issue related to the provision of confidential care for adolescents is the emergence and proliferation of health information technologies. While such platforms facilitate health care access and communication, they also create novel challenges to protecting the privacy of adolescents. Electronic health records (EHR) privacy controls cannot yet adequately address, let alone ensure, the confidentiality of adolescents. Patient portals available on most EHR platforms allow patients or caregivers to access to health information, including test results, diagnoses or problem lists, medications, and upcoming appointments. Few EHR platforms specifically protect confidentiality as a child moves into adolescence and becomes newly entitled to a private record. Moreover, sensitive health issues that an adolescent is not ready to disclose to others may be documented and accessed all too easily by other health professionals without explicit consent being given. Most EHR systems have not been designed to provide item-specific control over parental access and release of adolescent health care information. It is also costly for vendors to develop and maintain the levels of confidentiality mandated by law because they vary significantly according to jurisdiction^[27]. Clinicians are often left balancing their patient’s need for confidentiality with creating an accurate and complete medical record.

The SAHM and the AAP have both advocated for improved EHR technology to address these unique challenges^[28]^[29]. EHR patient portals generally do not yet have the technical capacity to maintain or support the ability of minors to give consent for health care, or to protect their sensitive health care information^[30]. The optimal solution would be to develop a separate portal for adolescents when they are deemed mature minors, but such transitional technologies are not readily available. HCPs should advocate for EHR program development to block sensitive results from appearing on any patient portal.

Telemedicine and related technologies are rapidly transforming the way clinical care is provided. Telemedicine is defined as a two-way live communication between patient and provider at a distant site that includes audio or video equipment (or both)^[31]. Telemedicine can improve health care access and is likely to be an increasingly common option for medical

interactions because it allows flexible scheduling. However, several barriers to privacy protection exist when telemedicine is compared with in-person visits. The need to establish and guarantee a private environment is a leading priority for HCPs using telemedicine [32]. In telemedicine visits, others may be present in-room but out of view, or sessions may be recorded without a patient’s knowledge or consent. Moreover, adolescents do not always have a private, quiet space at home to transmit from. HCPs can encourage adolescents to sweep the room with their cameras to establish who is present, to use headphones, or to utilize chat functions to limit the ability of others to overhear medical conversations. At times, the best strategy may be to encourage the adolescent to find a secure location outside of the home (e.g., an office at school) to speak from.

Health care provider comfort level

There is a wide range of understanding and practice regarding confidential care for adolescents in Canada [3]. Paediatricians and family physicians alike report having insufficient knowledge of requirements and have identified the need for additional training and resources [33]. Increasing education around privacy laws while reinforcing awareness of confidentiality concerns can improve knowledge gaps. Teaching on confidentiality should extend to all clinicians and front-line staff. Office staff should also be trained to welcome adolescents who present or call for an appointment on their own, and to safely relay test or other results.

Clinical setting

A broad range of facilitators and barriers to providing confidential care exist in different clinical settings (Table 1). Preventative health screening may be best addressed at routine health visits, but it is essential that HCPs create other opportunities to address confidential issues in various practice settings. Adolescents with higher levels of risk behaviours, (i.e., substance use or mental health issues) are more likely to use an emergency department (ED) as their primary source of care [34]. Equally, adolescents with chronic health conditions engage in risk behaviours at similar or even greater rates than healthier peers [35], making tertiary care encounters another option for screening and risk prevention in this population.

Studies have shown that adolescent patients are interested in being screened and receiving information on safe sexual practices and other risky behaviours in both ED [36] [37] and inpatient wards [38], regardless of gender, sexual experience, or relationship with primary care providers [39]. Developing protocols to optimize confidential care in various settings can mitigate obstacles such as time constraints, space limits, and insurance practices that may compromise confidentiality.

Table 1. Facilitators and barriers to providing confidential care for adolescents, by clinical setting

Clinical setting	Facilitators to confidential care	Barriers to confidential care	Strategies to improve confidential care
Outpatient clinic	Long-term, continuous relationship with a primary care provider Flexible clinical environment (i.e., designing waiting rooms to maximize privacy or creating and providing pertinent reading material) Continuity of care from a young age allows for early, anticipatory discussions with parents around the need for one-on-one time for the adolescent and HCP	Long-term relationship between parents and the adolescent's primary care provider may cast doubt on privacy protections Long periods in a waiting room can increase feelings of self-consciousness and vulnerability, and may expose them to encounters with peers	Establish an adolescent-friendly environment (i.e., flexible hours, targeted reading material and artwork) Post prominent reminders respecting need for private, confidential medical care Establish a multidisciplinary health care team to integrate multiple services in one location and maintain a single medical record
Emergency department (ED)	High patient volumes allow for broad access to adolescents from different backgrounds Adolescents with higher levels of risk behaviours are more likely to use an ED as their primary source of care and flag positive when screened	Time constraints, long wait times, and lack of private spaces can lead to missed screening opportunities Triaging is often conducted in the presence of a parent or caregiver	Protocols to ensure routine screening for risk behaviours in a private setting at time of triage Tools for promptly screening risky behaviours (i.e., ASQ-S, CRAFT, HEADS-ED)
Inpatient	Patients typically spend several days on an inpatient unit, allowing time for in-depth screening Adolescents with chronic health conditions may not access primary care providers when hospitalized, making tertiary care physicians an alternate form of screening	Family-centred rounds are part of standard care, but discussions and decision-making at bedside are not private Certain hospital settings do not offer single patient rooms, further limiting private bedside discussions Large number of team members on clinical teaching units	Elicit and work to adolescent preferences regarding scheduling confidential discussions outside of rounds and including a parent or caregiver Schedule follow-up discussions with a smaller, more personalized team

CRAFFT: Car, Relax, Alone, Forget, Friends, Trouble

HEADS-ED: Home, Education/Employment, Activities/peers, **D**rugs/alcohol, Suicidality

Emotions/behaviours/thought disturbance, **D**ischarge or current resources

Summary

Adolescents have a right to confidential care and private time with their HCPs, and clinicians are legally and ethically obligated to provide routine, private, confidential care to adolescent patients. Clinicians providing adolescent care must understand the importance of confidentiality, its limits, and strategies to best facilitate delivery of confidential care in the practice setting.

Recommendations for optimizing confidential care with adolescents

- HCPs must familiarize themselves with the federal and provincial or territorial legislation relating to health care privacy and confidentiality for their jurisdiction.
- HCPs should routinely counsel the adolescents they see in practice—and their parents or caregivers—about the meaning and importance of confidentiality, and any limits that may apply. These conversations ideally take place before the initial medical encounter to help mitigate any concerns.
- Beginning in early adolescence, HCPs should spend at least part of each health visit alone with an adolescent patient to convey that this is routine and valued health care practice. Clinicians should communicate to adolescents and their parents or caregivers the developmental importance of increasing autonomy and responsibility related to health care decision-making to facilitate better transition in navigating the adult health care system.
- HCPs are discouraged from asking in the presence of a parent or caregiver whether an adolescent would like time in private, because the adolescent may feel uncomfortable or reluctant to, agree.
- Medical providers must be aware of their own electronic health record (ERH) settings and limitations and should advocate for EHR program development to block sensitive results from appearing on any patient portal.
- Practice settings should review and revise their clinical procedures (including spacing limits, scheduling, charting) to ensure that adolescents' privacy and the confidentiality are fully protected. This could include posted documents describing patient rights and making sure families and clinical staff are familiar with and respect these rules.
- HCPs should have access to continuing education and training to ensure comfort and competence when providing confidential health care to adolescents at all stages in the patient journey. Teaching on confidentiality should extend to all front-line staff to ensure quality care for this population.

Acknowledgements

This position statement has been reviewed by the Acute Care, Bioethics, and Community Paediatrics Committees of the Canadian Paediatric Society, as well as by the CPS Paediatric Emergency Medicine Section Executive and members of the College of Family Physicians of Canada.

CANADIAN PAEDIATRIC SOCIETY ADOLESCENT HEALTH COMMITTEE (2021-2022)

Members: Holly Agostino MD, Marian Coret MD (Resident Member), Megan Harrison MD, Ayaz Ramji MD (Board Representative), Alene Toulany MD, Ashley Vander Morris MD, Ellie Vyver MD (Chair)

Liaisons: Amy Robinson MD (CPS Adolescent Health Section)

Principal authors: Holly Agostino MD, Alene Toulany MD

References

1. Sigman G, Silber TJ, English A, Epner JE. Confidential health care for adolescents: Position paper of the Society for Adolescent Medicine. *J Adolesc Health* 1997;21(6):408-15.
2. Thrall JS, McCloskey L, Ettner SL, Rothman E, Tighe JE, Emans SJ. Confidentiality and adolescents' use of providers for health information and for pelvic examinations. *Arch Pediatr Adolesc Med* 2000;154(9):885-92.
3. Wadman R, Thul D, Elliott AS, Kennedy AP, Mitchell I, Pinzon JL. Adolescent confidentiality: Understanding and practices of health care providers. *Paediatr Child Health* 2014;19(2):e11-14.
4. American Academy of Pediatrics; Committee on Adolescence. Achieving quality health services for adolescents. *Pediatrics* 2016;138(2):e20161347.
5. Ford C, English A, Sigman G. Confidential health care for adolescents: Position paper for the Society for Adolescent Medicine. *J Adolesc Health* 2004;35(2):160-67.
6. Klein DA, Paradise SL, Landis CA. Screening and counseling adolescents and young Adults: A framework for comprehensive care. *Am Fam Physician* 2020;101(3):147-58.
7. American College of Obstetricians and Gynecologists. Confidentiality in adolescent health care: ACOG Committee Opinion, Number 803. *Obstet Gynecol* 2020;135(4):e171-e177.
8. Berlan ED, Bravender T. Confidentiality, consent, and caring for the adolescent patient. *Curr Opin Pediatr* 2009;21(4):450-56.
9. Ginsburg KR, Slap GB, Cnaan A, Forke CM, Balsley CM, Rouselle DM. Adolescents' perceptions of factors affecting their decisions to seek health care. *JAMA* 1995;273(24):1913-18.
10. Fuentes L, Ingerick M, Jones R, Lindberg L. Adolescents' and young adults' reports of barriers to confidential health care and receipt of contraceptive services. *J Adolesc Health* 2018;62(1):36-43.
11. Ford CA, Millstein SG, Halpern-Felsher BL, Irwin CE. Influence of physician confidentiality assurances on adolescents' willingness to disclose information and seek future health care. A randomized controlled trial. *JAMA* 1997;278(12):1029-34.
12. White PH, Cooley WC, Transitions Clinical Report Authoring Group; American Academy of Pediatrics, American Academy of Family Physicians, American College of Physicians. Supporting the health care transition from adolescence to adulthood in the medical home. *Pediatrics* 2018;142(5):e20182587.
13. Government of Canada. Canada Health Act, RSC 1985, c C-6: <https://canlii.ca/t/532qv> (Accessed June 14, 2022).

14. Government of Canada. The Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. Office of the Privacy Commissioner of Canada. <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>. Published 2000. Accessed 12-11, 2020.
15. Government of Canada. Department of Justice. Article 12 of the Convention on the Rights of the Child and Children's Participatory Rights in Canada: <https://www.justice.gc.ca/eng/rp-pr/other-autre/article12/p3a.html> (Accessed June 14, 2022).
16. Légis Québec. Act Respecting Health Services and Social Services, chapter S-4.2: <http://legisquebec.gouv.qc.ca/en/showDoc/cs/S-4.2?&digest>. Published 1991. (Accessed June 14, 2022).
17. Government of Newfoundland and Labrador; Justice and Public Safety and Health and Community Services Departments. Advance Health Care Directives Act. SNL 1995 Chapter A-4.1: An Act Respecting Advance Health Care Directives and the Appointment of Substitute Health Care Decision Makers: <https://www.assembly.nl.ca/Legislation/sr/statutes/a04-1.htm>. Published 1999 (Accessed June 14, 2022).
18. Coughlin KW; CPS Bioethics Committee. Medical decision-making in paediatrics: Infancy to adolescence. *Paediatr Child Health* 2018;23(2):138-46: <https://cps.ca/en/documents/position/medical-decision-making-in-paediatrics-infancy-to-adolescence>.
19. Légis Québec. Civil Code of Québec, CCQ-1991: <http://legisquebec.gouv.qc.ca/en/showdoc/cs/ccq-1991> (Accessed June 14, 2022).
20. Canadian Medical Association. CMA Code of Ethics and Professionalism: <https://www.cma.ca/En/Pages/code-of-ethics.asp> (Accessed June 14, 2022).
21. Lim SW, Chhabra R, Rosen A, Racine AD, Alderman EM. Adolescents' views on barriers to health care: A pilot study. *J Prim Care Community Health* 2012;3(2):99-103.
22. McKee MD, O'Sullivan LF, Weber CM. Perspectives on confidential care for adolescent girls. *Ann Fam Med* 2006;4(6):519-26.
23. Toulany A, Katzman DK, Goldberg E, Matlow A, Kaufman M. Chaperoning adolescents: A bygone era or modern medical necessity? *Paediatr Child Health* 2012;17(6):305-06.
24. McKee MD, Rubin SE, Campos G, O'Sullivan LF. Challenges of providing confidential care to adolescents in urban primary care: Clinician perspectives. *Ann Fam Med* 2011;9(1):37-43.
25. Duncan RE, Vandeleur M, Derks A, Sawyer S. Confidentiality with adolescents in the medical setting: What do parents think? *J Adolesc Health* 2011;49(4):428-30.
26. American Academy of Pediatrics, Committee on Hospital Care and Institute for Patient- and Family-Centered Care. Patient- and family-centered care and the pediatrician's role. *Pediatrics* 2012;129(2):394-404.
27. Thompson LA, Martinko T, Budd P, Mercado R, Schentrup AM. Meaningful use of a confidential adolescent patient portal. *J Adolesc Health* 2016;58(2):134-40.
28. Society for Adolescent Health and Medicine; Gray SH, Pasternak RH, et al. Recommendations for electronic health record use for delivery of adolescent health care. *J Adolesc Health* 2014;54(4):487-90.
29. American Academy of Pediatrics, Committee on Adolescence; Council on Clinical and Information Technology; Blythe MJ, Del Beccaro MA. Standards for health information technology to ensure adolescent privacy. *Pediatrics* 2012;130(5):987-90.

30. Bourgeois FC, Taylor PL, Emans SJ, Nigrin DJ, Mandl KD. Whose personal control? Creating private, personally controlled health records for pediatric and adolescent patients. *J Am Med Inform Assoc* 2008;15(6):737-43.
31. Weinstein RS, Krupinski EA, Doarn CR. Clinical examination component of telemedicine, telehealth, mHealth, and connected health medical practices. *Med Clin North Am* 2018;102(3):533-44.
32. Barney A, Buckelew S, Mesheriakova V, Raymond-Flesch M. The COVID-19 pandemic and rapid implementation of adolescent and young adult telemedicine: Challenges and opportunities for innovation. *J Adolesc Health* 2020;67(2):164-71.
33. Riley M, Ahmed S, Reed BD, Quint EH. Physician knowledge and attitudes around confidential care for minor patients. *J Pediatr Adolesc Gynecol* 2015;28(4):234-39.
34. Wilson KM, Klein JD. Adolescents who use the emergency department as their usual source of care. *Arch Pediatr Adolesc Med* 2000;154(4):361-65.
35. Surís JC, Michaud PA, Akre C, Sawyer SM. Health risk behaviors in adolescents with chronic conditions. *Pediatrics* 2008;122(5):e1113-18.
36. Mollen CJ, Miller MK, Hayes KL, Wittink MN, Barg FK. Developing emergency department-based education about emergency contraception: Adolescent preferences. *Acad Emerg Med* 2013;20(11):1164-70.
37. Fine LC, Mollen CJ. A pilot study to assess candidacy for emergency contraception and interest in sexual health education in a pediatric emergency department population. *Pediatr Emerg Care* 2010;26(6):413-16.
38. Ross AM, White E, Powell D, Nelson S, Horowitz L, Wharff E. To ask or not to ask? Opinions of pediatric medical inpatients about suicide risk screening in the hospital. *J Pediatr* 2016;170:295-300.
39. Guss CE, Wunsch CA, McCulloh R, Donaldson A, Alverson BK. Using the hospital as a venue for reproductive health interventions: A survey of hospitalized adolescents. *Hosp Pediatr* 2015;5(2):67-73.

Disclaimer: The recommendations in this position statement do not indicate an exclusive course of treatment or procedure to be followed. Variations, taking into account individual circumstances, may be appropriate. Internet addresses are current at time of publication.