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

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

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

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

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

David Goodis, Advisor
INQ Consulting
dgoodis@inq.consulting

P. O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 • Facsimile: (709) 729-6500
E-mail: commissioner@oipc.nl.ca • www.oipc.nl.ca

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. Anecdotally 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.