ATIPP Office supplemental submission to the ATIPPA, 2015 Review Committee (on behalf of Minister responsible for the administration of the Act)

May 2021

Table of Contents

Introduction

As noted in our original submission from November, 2020, the Minister of the Department of Justice and Public Safety is the Minister responsible for the administration of the **Access to Information and Protection of Privacy Act, 2015** (the Act). The ATIPP Office assists with this mandate. In this capacity, our Office provided a submission to the Review Committee outlining various suggestions for ways to enhance the provisions of the Act.

Since then, our Office has had the opportunity to review submissions made by various stakeholders. In these submissions are common themes, many of which were included in our original submission. Given our mandate, which supports the Minister responsible for the administration of the Act, we felt it would be beneficial to discuss in detail some of the suggestions put forth by other stakeholders for your consideration.

Topic brought forward by other stakeholders

1. Definitions/provisions from PHIA – general comments

Issue

The OIPC has put forward several recommendations based on definitions/provisions found within the **Personal Health Information Act** (PHIA). While there may be merit with updating the privacy provisions of the Act, our Office has some concerns with amendments being made based on provisions found within PHIA.

Personal health information is widely recognized as highly sensitive personal information. There is also a necessity for health professionals to share information within the circle of care. The unique nature of personal health information has led to most jurisdictions within Canada (including this province), introducing or planning to introduce legislation specific to this sub-category of personal information.

The creation of PHIA was in recognition of the fact that personal health information, as a subcategory, requires a higher threshold of protection and potentially more flexibility in regards to sharing within the circle of care. Furthermore, PHIA is unique in that it encompasses both public bodies and other non-public body health care providers that do not fall under the Act.

Additionally, it was recognized that the provisions of PHIA should prevail over the Act, which is reflected in section six of the Act:

Relationship to Personal Health Information Act

6. (1) Notwithstanding section 5, but except as provided in sections 92 to 94, this Act and the regulations shall not apply and the *Personal Health Information Act* and regulations under that Act shall apply where

(a) a public body is a custodian; and

(b) the information or record that is in the custody or control of a public body that is a custodian is personal health information.

(2) For the purpose of this section, "custodian" and "personal health information" have the meanings ascribed to them in the *Personal Health Information Act*.

In their 2004 Guide to the Personal Health Information Protection Act, The Ontario Information and Privacy Commissioner notes:

> The rules recognize the unique character of personal health information – as one of the most sensitive types of personal information that is frequently shared for a variety of purposes, including care and treatment, health research, and managing our publicly funded health care system.

In their Special Report – A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector, the Information and Privacy Commissioner also noted:

> Personal health information that is collected by health care providers in the delivery of health care is extremely sensitive. Arguably, it is the single most sensitive type of personal information. It encompasses information about:
>
> - the physical, mental and emotional status of individuals over their lifetime;
> - lifestyle and behaviour;
> - health conditions and concerns;
> - history of health care procedures and medication use;
> - results of medical tests;
> - related information about family members and other individuals; and
> - genetic information about individuals and their blood relatives.
>
> …Given these characteristics of personal health information, health sector privacy is considered to be unique.

This characterization is further supported by the Department of Health and Community Services' (HCS) 2008 news release regarding PHIA in which they note:

> "An individual's health record is perhaps the most sensitive of all personal information, which is why it is imperative that we take measures to ensure its protection for our residents," said the Honourable Ross Wiseman, Minister of Health and Community Services. "This legislation clarifies the appropriate balance between protecting individual privacy and using personal health information for legitimate reasons. This becomes increasingly important as we move forward with the development of integrated Electronic Health Records to better manage an individual's health care.

While PHIA applies to various types of health care providers, it is only in relation to a specific sub-category of personal information (i.e. personal health information) which lends itself to being more prescriptive than the Act, which applies to all personal information in the custody or control of public bodies. These public bodies have varying mandates, and as a result, the scope and type of personal information in their custody or control varies vastly. The recommendations put forward by the OIPC do not appear to recognize this distinction between PHIA and the Act. While it is possible that provisions within PHIA may be applicable to some of the personal information that public bodies have in their custody or control, it is highly unlikely that they would apply to all personal information, including that which is not overly sensitive or may not be considered an unreasonable invasion of privacy under the Act (e.g. permit applications, names and contact information in a business context, etc.).

The privacy provisions of the Act are based on reasonableness. It would not be reasonable by any standard to expect the same level of protection for a moose-hunting permit as a mental health referral.

Suggestions

For the reasons outlined above, our Office suggests that the Committee not adopt provisions from PHIA as amendments to the Act.

Alternatively, if the Committee determines that amendments to the Act based on recommendations put forward by the OIPC in relation to PHIA are appropriate, our Office would suggest that the Committee consider modifying any provisions from PHIA to include a “reasonableness” clause.

2. Legislative requirement for policies/procedures

Issue

The OIPC has recommended that there be a legislative requirement to develop information policies and procedures.

Suggestions

As noted in the section above, our Office suggests that the Committee should not adopt provisions of PHIA as amendments to the Act. However, if the Committee determines that it would be appropriate to legislate the requirement for policies/procedures, our Office would suggest that the Committee consider any such amendment to be based on reasonableness, which would be in line with other provisions of the Act. In most instances, a general, overarching privacy policy should be sufficient, with additional procedures developed where necessary. It should only be in circumstances where the general policy, and additional procedures unique to a specific program, are not

reasonably sufficient that additional policies should be developed – this can be identified through a privacy assessment.

To that end, our Office has a Protection of Privacy Policy and Procedures Manual. This policy and procedures manual outlines how personal information is to be collected, used, disclosed, accessed, etc., and includes a detailed privacy breach protocol. This applies to all government departments and is available to any other public body that wishes to adopt or modify it for their purposes.

We are concerned that if there is a requirement for a new policy on every program or service, it will be difficult for employees to learn, understand and apply each policy effectively. It would also make it difficult to train employees in relation to all of the varying policies. Currently, if an employee inadvertently sends an email to the wrong person, the same advice about how to handle the privacy breach should apply, regardless of which program or project they work for. However, if there is a specific policy for each program/service, there could be variations which impact how to proceed.

Our Office is not arguing that there are no circumstances under which a separate policy would be appropriate; there are absolutely situations where a program collects uniquely sensitive information or has substantially different processes or structures that have privacy implications which are not sufficiently mitigated by a general, overarching policy and specific procedures. We simply do not think that this is the case for every program or service that public bodies provide.

If potential amendments included a "reasonableness" provision, it would ensure that the provisions were not interpreted to require a specific privacy policy for every service/program that is offered by a public body, therefore, saturating the public body with similar and unnecessary policies and procedures. For example, it would not be reasonable to expect a public body to create a policy regarding the collection of personal information for the purpose of moose hunting permits. The collection, use, disclosure, access, etc. of any personal information in relation to that permit would fall under the general privacy policy, and any unique procedures that may be required.

3. Privacy Impact Assessments

Issue

The OIPC has recommended that the definition of a privacy impact assessment be amended.

Our Office has developed various tools to assess programs/services, including a short-form PIA called a preliminary privacy impact assessment (PPIA). In many instances this

short-from PIA is able to be used rather than a full PIA. While it is not the primary purpose of the PPIA, one of its elements is determining whether a full PIA is required.

Suggestion

If the Committee amends the definition of privacy impact assessment, consideration be given to ensure the definition is broad enough to continue to encompass the preliminary privacy impact assessment.

4. Common or integrated programs

4.1 Definition of a common or integrated program

Issue

The OIPC has recommended that a definition of a common or integrated program be added to the Act, and that it be based on the definition found in British Columbia's **FIPPA**.

In their submission, the OIPC referred to the difference between our Office and theirs in terms of the definitions we have adopted for common or integrated programs. The matter of common or integrated programs were first brought forward during the 2010 ATIPPA Review completed by Commissioner John Cummings. At that time it was noted that the primary purpose for this provision was to allow for the sharing of personal information between entities providing common programs/services in instances where it otherwise would not be authorized under the privacy provisions of the Act – if there was already authority (i.e. the individual had consented) there would be no requirement to rely on this provision.

In his 2011 final report, Review of the Access to Information and Protection of Privacy Act, Commissioner Cummings noted:

> I think the regime created under ATIPPA is too rigid in terms of the restrictions it places on the legitimate use of personal information, such as those referred to above. It should be relaxed to permit greater scope for such legitimate use. I think Alberta has created the best regime for incorporating greater flexibility and their model should be adopted in this province.

In reviewing legislation and policies within Canada relating to common or integrated programs, our Office determined that the definition that would best reflect the realities of how public bodies work within this province would be the definition found in Alberta FOIP Bulletin No. 8:

> A "common or integrated program or service" means a single program or service that is provided or delivered by two or more public bodies. The program or service may have several distinct components, each of which is provided or delivered by a separate public body. These components together comprise the common program or integrated service.

Our Protection of Privacy Policy and Procedures Manual, adds further clarity:

> Each public body partner must be integral to the program or service. For example, a nursing practicum program requires the participation of both the post-secondary institution, and the health care body; the program would not function without the services of each body. Public bodies may have clients in common, but that factor alone does not make a program or service common or integrated.

One of the primary factors that contributed to our Office relying on this definition was the role the Office of the Chief Information Officer has within government. While some programs/services they provide are being brought forward by OCIO in concert with other departments, and would therefore be common or integrated programs, in most instances, they are simply providing a service to their clients (i.e. departments), similar to the function that many IT divisions within other public bodies provide (e.g. Memorial University, NL Housing, etc.).

In this capacity, OCIO assists government departments with providing programs and services, however, they are not provided or delivered by OCIO. There are other departments/divisions within Government that have similar roles. For example, The Public Engagement Division of the Communications and Public Engagement Branch, often assists departments with public engagement initiatives.

If the definition the OIPC is recommending is adopted, it would essentially result in any assistance that these government entities provide to other government department being considered a common or integrated program. This does not appear to be within the spirit of the legislation or the purpose for which subsection 68(1)(u) was adopted.

It is also worth noting that in their 2014 review of the Act, The ATIPPA Review Committee had clearly reviewed our policy manual in relation to common or integrated programs, as it evidenced in their report where they note the "manual gives guidance as to what should be done to prepare for a common or integrated program or service." At no point in their report did they question the definition that our Office had used in relation to common or integrated programs.

Suggestions

If the Committee determines it appropriate to include a definition for a common or integrated program within the Act, our Office would suggest consideration be given to adopting the definition this Office relies on.

Alternatively, if the Committee determines that the definition recommended by the OIPC is appropriate, we would suggest consideration be given to adding provisions to the Act noting that where a department (e.g. OCIO, CPEB) is providing purely support services to a client department those services do not fit within the definition.

4.2 Requirement for ISAs for every common or integrated program (s.72)

Issue

The OIPC has recommended that section 72 be amended to add a requirement for an information sharing agreement (ISA) to be completed by parties to a common or integrated program or service. This, in conjunction with their recommendation regarding the definition for a common or integrated program, would result in ISAs being required in any instance where a department such as OCIO or CPEB provides support services to a client department. Such a requirement would appear to be unwarranted and unnecessarily increase the administrative burden of the Act.

Suggestions

Our Office would suggest that the Committee consider whether it is necessary to include a legislative requirement for ISAs to be completed for every common or integrated program. The determination of whether an ISA should be completed can be made during a privacy assessment, which the OIPC has recommended encompass all public bodies other than municipalities.

If the Committee determines that it is appropriate to amend the Act to include a requirement for ISAs, in addition to adopting the OIPC's recommended definition of a common or integrated program, our Office would suggest that consideration be given to include limitations to the circumstances under which ISAs are required, including, but not limited to:

- ISAs are not required for programs/services that fit under the definition of a common or integrated program in name only (e.g. where OCIO or the Public Engagement (PEP) are providing their clients with support only, etc.);
- ISAs are not required where disclosure is authorized under a paragraph of 68 other than 68(1)(u), except in cases where other factors weigh in favour of signing an ISA (e.g. sensitivity of personal information, etc.).
- ISAs are not required where the type of personal information being collected, used or disclosed, does not warrant an ISA, as determined through a privacy assessment.

As noted above, the assessment of whether an ISA is required can be completed during a privacy assessment and would be in line with the privacy provisions that are based on reasonableness.

5. Mandatory disclosure when in the public interest (s.9)

Issue

Subsection 9(3) of the Act states:

> Whether or not a request for access is made, the head of a public body shall, without delay, disclose to the public, to an affected group of people or to an applicant, information about a risk of significant harm to the environment or to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.

In their submission, the OIPC is recommending that subsection 9(3) be amended to "to remove the potential for limitation of its applicability to matters that are 'urgent' as a temporal consideration." They put forth this recommendation, in part, due to the fact that:

> One could imagine a threat to health, safety or environmental harm that was gradually emerging and it was in the public interest to have this information disclosed before the matter became urgent. The need to have evidence that clearly demonstrates the risk of harm necessarily implies that urgency is one of the considerations, but we recommend that the section be clarified to avoid automatically excluding cases that do not have immediacy of risk as a fundamental feature.

Suggestion

Our Office would suggest that the Committee consider whether it would be more appropriate to put this forward as a recommendation for government to consider rather than a recommendation for amendment.

In addition to further analysis, it would be necessary for clear guidance to be developed on how a public body would be able to determine at what point an emerging issue would require disclosure under this Act, if not based on urgency. For example, would this only be in circumstances where other legislation or processes do not require similar disclosure, engagement, etc.

Any analysis on this recommendation would require consultation with other public bodies, stakeholders, etc. that are experts in other legislation and familiar with disclosure requirements outside of this Act.

6. OIPC Complaint process

6.1 Clarification re: process

Issue

A number of public bodies brought forward recommendations regarding the OIPC and their investigatory functions. Since our submission in November, 2020, our Office has become aware of a number of concerns with the complaint process that would be in line with the recommendations brought forward. Of particular concern, is the process when an investigation moves from the informal to formal investigation stage.

Prior to 2015, public bodies were able to provide formal submissions to the OIPC once a formal investigation was initiated, as the matter was unable to be resolved informally. This afforded the public body, and presumably the complainant, the opportunity to provide a final summary of their positions, which may include additional information that only became relevant during the informal investigation stage.

However, since 2015, in order to meet their legislated timelines, the OIPC has changed their process significantly, including the process for public bodies to provide a response regarding a complaint. Generally speaking, submissions must be provided within the first 10 business days of notification of the complaint, when it is still in the informal resolution stage.

It has been our experience that there is communication through the informal stage of the investigation. The OIPC provide their general findings and provide the public body, and presumably the complainant, the opportunity to respond in an effort to resolve the matter before requiring a formal investigation. However, it appears that once the informal stage of the investigation has completed that the level of communication varies. While in some cases there could be additional communication, there have been cases where there is no communication with the public body until the final report is issued. This is of particular concern in cases where the OIPC appears to agree with the position of the public body toward the end of the informal stage and has indicated they will try to resolve the matter informally. However, without any further communication, the public body receives the final report in which the OIPC has taken a different position on the matter.

The Act is extremely prescriptive when it comes to public body requirements, however, does not appear to hold the OIPC to the same standard in terms of documentation and communication during the complaint process.

Suggestion

Consider amending the provisions regarding the complaint process with the OIPC. For example, if a complaint cannot be resolved informally and it moves to the formal investigation stage, it should be mandatory for the OIPC to notify the public body and complainant and opportunity be provided to both parties to provide additional submissions prior to the final report being issued.

Additionally, the OIPC should be legislatively required to provide the public body and the complainant with their general findings during the informal stage of the complaint, to ensure both parties have sufficient information when completing their final submission (if the suggestion above is made). This is of particular importance in cases where the OIPC has indicated that they agree with a party's position, but then issue a report that takes the opposite or varying position.

6.2 Authority to not investigate a complaint

Issue

Sections 45 and 75 of the Act provide the OIPC with the discretion to not investigate a complaint under specific circumstances. The City of Corner Brook has recommended that these provisions be amended to be mandatory rather than discretionary.

Our Office is aware of an instance where a complaint was received where the individual was unable to provide specific details or any supporting documentation other than a statement that they thought someone in a public body had inappropriately breached their privacy four or five years ago. This complaint was forwarded to the public bodies they had identified as potentially breaching their privacy, without any further questions or follow-up with the complainant.

With such limited details, it was extremely difficult for the public bodies to determine whether the individual's privacy had been breached, and provide the OIPC with the level of detail they require within 10 business days. One question brought forward by one of the public body's was whether the OIPC had contacted the complainant, or anyone else with supporting information to confirm whether a breach had even occurred. They did not, but rather accepted the complaint and forwarded to the public bodies prior to obtaining sufficient details to allow the public bodies to fully investigate the matter or respond to the complaint in a meaningful way.

If similar complaints continue to occur, with limited details being provided to the public body, the coordinator may be required to consult more staff than necessary in order to determine to what the individual's complaint is in relation. This would impact the number of people to whom the complaint is disclosed. This potential for

unnecessary disclosure would be mitigated if public bodies were only notified of the complaint once the OIPC obtained sufficient details for them to respond.

Our Office recognizes that complainants are unlikely to be fully versed in privacy legislation and requirements, and may need the OIPC to assess whether a complaint is warranted. As such, complainants should not be expected to have detailed arguments prepared about how the law was not followed. However, complainants should be able to provide sufficient factual details to assess the complaint. If they do not have these details, the onus should be on the OIPC to either use their discretion not to investigate or to work with the complainant to obtain sufficient details, which may include obtaining their consent to contact others who may be able to assist in the matter. Furthermore, this should be done prior to notifying a public body.

Suggestion
Consider whether to amend the Act to require the OIPC to communicate with the complainant and receive sufficient details to proceed prior to sending the notification to the public body.

6.3 Time limit for responding to a complaint (s.46)

Issue
The College of the North Atlantic recommended that the timeframe set out in section 46 be extended beyond 65 days, while Tourism, Culture, Arts and Recreation suggested the 10 day timeframe provided to public bodies to respond to complaints be extended.

Suggestion
As noted above, the current policy of the OIPC is to provide public bodies with 10 business days to respond to a complaint once notified. If the Committee determines that extending the timeframe for an OIPC investigation is appropriate, we would suggest that consideration be given to amending the Act to provide provisions outlining the timeframe allotted to public bodies and complainants to respond to a complaint in both the informal and formal stages of the investigation. Furthermore, if the timeframe is extended, and provisions regarding the above are added, the timeframe for responding should be greater than 10 business days.

7. Publication Scheme (s.111)

In their submission, the OIPC has brought forward numerous recommendations regarding publications schemes, the majority of which focus on oversight by their Office.

This section will review the standard template required by subsection 111(1) and some of the recommendations made by the OIPC.

7.1 Standard template

Issue

In their submission the OIPC noted that subsection 111(1) required their office to create a standard template for the publication scheme, which they advised was completed in January, 2016. At this time, the OIPC published an overview of the legislative requirements set out in section 111, and what their expectations would be. After the overview was published our Office met with the OIPC to discuss best steps moving forward. At this time, we questioned whether they were planning to update their guide to include a standard template for public bodies to adapt and use for their purposes, as required by subsection 111(1). The OIPC advised that they would not be developing a standard template as they felt it would be too prescriptive.

For this reason, our Office moved forward with developing a guide for public bodies, including a basic outline for a webpage, to provide some guidance on what a publication scheme may look like. Based on the assumption that government departments would be the first public bodies added to the regulations, it was developed in consultation with ATIPP Coordinators and IM professionals within government, and sent to the OIPC for review. A standard template was not developed at this time, given consultations with OCIO and CPEB (which is responsible for the government website) had not yet occurred. Given much of the information required under section 111 is currently available on the government website (and likely on other public body websites), we felt it would be necessary to consult with these entities to determine the best way to ensure duplication did not occur which may lead to inconsistencies and impact the overall functionality of the government website.

It is our belief that the guide we have developed is in compliance with the legislation and OIPC expectations. However, based on these requirements, in particular the level of detail required relating to personal information banks, it is our belief that it is not overly user-friendly, which may inhibit its usefulness.

Suggestions

- Consider whether a publication scheme, as currently outlined in section 111 is necessary. If it is deemed necessary, consider amendments to make it more user friendly. Additionally, consider whether provisions could be added to eliminate the requirement for public bodies to include information already publicly available in the publication scheme (e.g. mandate, divisions/branches, etc.).

- If it is determined that section 111 should not be modified, consider whether it would be appropriate to require the OIPC to develop a standard template in compliance with subsection 111(1) that will be prescriptive and can then be easily adapted by public bodies as intended.
- If it is deemed necessary for the OIPC to develop a standard template in compliance with subsection 111(1), consider whether it would be appropriate to require them to consult with, at minimum, the following stakeholders within affected public bodies prior to finalization:
    - IM professions;
    - IT professionals;
    - Divisions responsible for the overall design and function of the public body website;
    - ATIPP coordinators; and
    - Any other stakeholders deemed appropriate by the Committee.

7.2 Requirement for public bodies to submit a publication scheme to the OIPC for review and comment

Issue

The OIPC has recommended that a requirement be added to section 111 that public bodies must submit a completed publication scheme to the Commissioner for review and comment.

Suggestions

Consider whether this is necessary. If a standard template is developed in consultation with public bodies, this recommendation would appear unnecessary. Furthermore, there is nothing in the legislation that would preclude the OIPC from reviewing publication schemes once they are published.

7.3 OIPC Authority to require deficiencies to be addressed

Issue

The OIPC has recommended that a requirement be added to provide the Commissioner with authority to require any deficiencies in the publication scheme to be addressed within a reasonable period of time to be determined by the Commissioner.

Suggestions

Our Office would suggest consideration be given to whether this is necessary. If a standard template is developed in consultation with public bodies, this recommendation would appear unnecessary. Alternatively, if the Committee considered it appropriate to amend the legislation as recommended by the OIPC, we would suggest consideration be given to modifying proposed amendments by

allowing the OIPC the ability to make recommendations regarding the publication scheme (once it is published) which the public body can consider but is not legislatively required to comply with.

Conclusion

Our Office appreciates the opportunity the Committee has afforded us to provide a supplemental submission in relation to other stakeholder submissions. We feel, given the mandate of our Office, our knowledge of the Act, privacy principles, court and OIPC decisions, directives, etc. across Canada and other jurisdictions, and our extensive experience supporting public bodies that fall under the Act, we are in a unique position. This position affords us the ability to recognize the administrative and procedural implications of recommendations put forward in submissions that other stakeholders may not be aware of or interested in. While our Office supports legislative amendments that will forward the principles and spirit of the Act, we recognize, that the Act does not stand on its own, and must be considered in the context of this province and the public bodies (and staff) which must uphold it.

We would be happy to discuss our submission further, or any other submissions if the Committee feels it would be of any benefit.