

**2017 REVIEW OF  
THE FREEDOM OF INFORMATION  
AND PROTECTION OF PRIVACY ACT (FIPPA)  
COMMENTS FROM MANITOBA OMBUDSMAN**

Manitoba  Ombudsman

## TABLE OF CONTENTS

<b>Introduction</b>	<b>3</b>
<b>1. Duty to Document</b>	<b>4</b>
<b>2. Proactive Disclosure</b>	<b>6</b>
<b>3. Access to Information – Procedural Matters</b>	<b>8</b>
Application for Access Form	8
Requests That involve Personal Health Information to Which PHIA Applies	9
Abandoned Requests	10
Fees	11
Fee Waivers	13
Notice to an Applicant and a Third Party Consulted Under Section 33	14
<b>4. Access to Information – Exceptions to Access</b>	<b>16</b>
Privacy of a Third Party	16
Business Interests of a Third Party	18
Labour Relations Interests of a Public Body as Employer	20
Cabinet Confidences	22
Advice to a Public Body	25
Information That Will be Made Available to the Public	28
Public Interest Override for Exceptions	29
<b>5. Protection of Privacy</b>	<b>30</b>
Protection of Personal Information	30
Mandatory Breach Notification	32
Secure Destruction of Personal Information	33
Correction of Personal Information	33
No Adverse Employment Action	35
Big Data Analytics	36
<b>6. Oversight Role of the Ombudsman</b>	<b>37</b>
Rename Title to Information and Privacy Commissioner	37
Powers of the Ombudsman Concerning Audits	38
Production of Records Over Which Solicitor-Client Privilege is Claimed	39
Complaint Form	42
Additional Complaint About a Failure to Protect Personal Information	42
Interjurisdictional Investigations	43
Disclosures by Ombudsman	44
Ombudsman’s Right to be a Party to Adjudicator’s Review	45
Ombudsman’s Right to Intervene as a Party to an Appeal	45
<b>7. Role of the Information and Privacy Adjudicator</b>	<b>46</b>
Adjudicator’s Orders	46
<b>8. Other Issues</b>	<b>48</b>
Additional Offences	48
Time Limit for Starting a Prosecution	49
Review Period	49
<b>Summary of Recommendations to Amend FIPPA</b>	<b>51</b>

## INTRODUCTION

The Freedom of Information and Protection of Privacy Act (FIPPA) provides Manitobans with important rights concerning information held by public bodies, including their own personal information (PI). FIPPA came into effect on May 4, 1998, for provincial departments and agencies, on August 31, 1998 for the City of Winnipeg and on April 3, 2000, for local public bodies, including local government bodies, educational bodies and health-care bodies.

FIPPA provides a right of access to information held by public bodies, subject to limited and specific exceptions set out in the act. The right of access is broad to facilitate openness and transparency. Access to information enables citizens to scrutinize decisions and actions of public bodies to ensure that public bodies are accountable to the citizens they serve.

With respect to PI, FIPPA provides individuals with a right of access to their own PI and a right to seek a correction to PI where there is an error or omission in the information. FIPPA provides a right to privacy by setting out rules that restrict how public bodies collect, use, disclose, protect and retain PI.

The right of complaint to the ombudsman enables access to information applicants to seek an independent review of how public bodies have responded to their access requests for general information or their own personal information. FIPPA also provides individuals with a right to make privacy complaints about how public bodies have handled their PI.

Since 2004, when FIPPA was last reviewed, many changes have occurred to the way in which information is collected, stored, used, disclosed and managed. While paper records continue to be used, many public bodies have transitioned to electronic records or a hybrid system. The increased use of technology has a significant impact on access and privacy rights. Increasingly, public bodies make information available to the public on their websites. Electronic systems that collect, use and disclose PI can facilitate efficiency and enable innovation, but risks to PI need to be carefully assessed and managed in an electronic information environment.

Access and privacy laws across Canada and around the world are based on internationally recognized fair information practices. This foundation creates many similarities, particularly across Canada, which also facilitates comparisons of differences in provisions between laws.

FIPPA requires that a comprehensive review of the operation of the act, which involves public representations, be conducted. Further to a public review of FIPPA in 2004, the act was significantly amended in 2011. Periodic reviews of FIPPA are essential to examine if the law is operating as intended and to ensure that the law is updated.

Manitoba Sport, Culture and Heritage published a discussion paper, [\*A Review of The Freedom of Information and Protection of Privacy Act: Tell Us What You Think\*](#), on March 29, 2017, which highlights and invites comments on various issues. Many of our comments about FIPPA relate to questions raised in the discussion paper.

## 1. DUTY TO DOCUMENT

### Issue

Access to information rights depend on public bodies documenting their key decisions and actions. There should be a requirement set out in legislation that creates a duty to document to ensure that citizens have a meaningful and effective right of access.

### Discussion

In 2016, the information and privacy oversight offices across Canada, including Manitoba Ombudsman, issued a joint statement that called on governments to:

Create a legislated duty requiring all public entities to document matters related to their deliberations, actions and decisions. This duty must be accompanied by effective oversight and enforcement provisions to ensure that Canadians' right of access to public records remains meaningful and effective.

A duty to document would ensure that records explaining the basis for decisions are created and are therefore subject to access under FIPPA. However, having adequate documentation also facilitates evidence-based decision making within public bodies. Documenting key decisions and actions is a responsible administrative practice that promotes accountability, good governance and public trust. A meaningful and enforceable duty to document depends on independent oversight.

A duty to document could be incorporated into existing information management laws or FIPPA. With respect to government records management legislation, the Archives and Recordkeeping Act recognizes the importance of good recordkeeping and it also sets out prohibitions and penalties regarding certain actions relating to government records, as follows:

#### **Prohibition re government record**

**28(1)** No person shall, with an intent to deprive the government, a government body, or the archives, of the custody, control, use of or access to a government record,

- (a) destroy or damage a government record;
- (b) erase or remove information from a government record or make a government record illegible;
- (c) remove or conceal a government record from the government, a government body or the archives; or
- (d) direct, counsel or cause any person in any manner to do anything mentioned in clause (a), (b) or (c);

except as provided in a records schedule approved under this Act.

#### **Exception**

**28(2)** Subsection (1) does not apply to a person who retains or destroys a government record in accordance with

- (a) *The Financial Administration Act* or a regulation under that Act;
- (b) *The Real Property Act* or *The Registry Act*; or
- (c) an enactment of the federal government.

**Offence**

**28(3)** A person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of not more than \$50,000.

**Prosecution within two years**

**28(4)** A prosecution under subsection (1) may be commenced not later than two years after the day the alleged offence was committed.

An option could be to legislate a duty to document within information management legislation such as the Archives and Recordkeeping Act, and then expand subsection 28(1) to include a prohibition relating to an intent to deprive the government, a government body, or the archives, of the custody, control, use of or access to a government record, by failing to create the record as required under that act. Similar changes would be required with respect to information management requirements that apply to public bodies to which the Archives and Recordkeeping Act does not apply.

If there was a duty to document set out under the Archives and Recordkeeping Act or any other such law or by-law of a local public body, this duty to create a record could be subject to investigation under FIPPA. The ombudsman already has the power under FIPPA to conduct an investigation to ensure compliance with requirements respecting the security and destruction of records set out in the Archives and Recordkeeping Act or other such laws:

**General powers and duties**

**49** In addition to the Ombudsman's powers and duties under Part 5 respecting complaints, the Ombudsman may

- (a) conduct investigations and audits and make recommendations to monitor and ensure compliance
  - (i) with this Act and the regulations, and
  - (ii) with requirements respecting the security and destruction of records set out in any other enactment or in a by-law or other legal instrument by which a local public body acts;

If information management laws such as the Archives and Recordkeeping Act were amended to legislate a duty to document, subclause 49(b)(ii) above could be amended to include "creation" as follows:

- (ii) with requirements respecting the creation, security and destruction of records set out in any other enactment or in a by-law or other legal instrument by which a local public body acts;

**Recommendation 1**

There should be a legislated duty requiring public bodies to document matters related to their deliberations, actions and decisions. This duty could be incorporated into information management laws and subclause 49(a)(ii) of FIPPA should be amended to enable the ombudsman to investigate compliance with requirements respecting the creation, security and destruction of records set out in any other enactment or in a by-law or other legal instrument by which a local public body acts. Alternatively, FIPPA could be amended to create a duty to document.

## 2. PROACTIVE DISCLOSURE

### Issue

Proactive disclosure (without the need to make an application for access under FIPPA), makes information available to the public, usually through websites of public bodies. Consideration should be given to whether amendments to FIPPA could increase and strengthen proactive disclosure and open government initiatives.

### Discussion

Proactive disclosure of information can have several benefits, including the potential to reduce reliance and pressure on FIPPA's access to information system, to enable citizens to become better informed about and engaged with the public bodies that serve them, and to promote openness and accountability of public bodies.

Section 76 of FIPPA enables public bodies to identify types of records and make them available to the public without requiring an access application under FIPPA, as follows:

#### **Records available without an application**

**76(1)** The head of a public body may specify records or categories of records that are in the custody or under the control of the public body and that are available to the public without an application for access under this Act.

#### **Fee**

**76(2)** The head of a public body may require a person who asks for a copy of a record available under subsection (1) to pay a fee to the public body, unless such a record can otherwise be accessed without a fee.

Amendments to FIPPA that came into effect in 2011 set out certain records that the provincial government must make available to the public:

#### **Ministerial expenses available to public**

**76.1(1)** The government shall make available to the public a summary of the total annual expenses incurred by each member of Executive Council for the following:

- (a) transportation and travel;
- (b) accommodation and meals;
- (c) promotion and hospitality;
- (d) cell phone and personal electronic communication devices.

#### **Summary to cover fiscal year**

**76.1(2)** The summary is to cover the period beginning on April 1 of one year and ending on March 31 of the following year, and must be made available within four months after the end of each fiscal year.

#### **Definition of "expenses"**

**76.1(3)** In this section, "**expenses**" means costs

- (a) that the member incurs personally while performing the responsibilities of his or her office; and
- (b) that are paid for through the department over which the member presides.

The provincial government has amalgamated information on its [proactive disclosure website](#), which includes the above as well as other information, such as:

- information on government contracts valued at \$10,000 or more
- mandate letters
- cabinet orders-in-council
- weekly listings of access requests received
- departmental reports and statistics
- transition materials to brief new government ministers

Reports, studies and other documents are often produced electronically and posting them on websites would be relatively straightforward. To expand proactive disclosure, consideration should be given to whether a legislative amendment is necessary or whether this could be achieved through policies. Proactive disclosure efforts can at times face challenges in determining which records to post. The privacy of identifiable individuals needs to be carefully considered in order to prevent the unauthorized disclosure of personal information. Developing a strategy that includes consultation with stakeholders can be effective in monitoring and measuring progress.

A paper-based format of proactive disclosure had been required under the former section 75 of FIPPA, which was repealed following the 2004 review of the act. It had required a directory to be maintained to assist people in identifying and locating records held by public bodies, as follows:

#### **Directory**

**75(1)** The responsible minister shall

- (a) prepare a directory to assist in identifying and locating records in the custody or under the control of public bodies;
- (b) make every reasonable effort to ensure that the directory is kept up to date;
- (c) ensure that copies of the directory are made available to public bodies; and
- (d) ensure that copies of the directory are available to the public through libraries and electronic information networks.

#### **Contents of directory**

**75(2)** The directory must include

- (a) a description of the mandates, functions and organization of each public body;
- (b) a description of records, including personal information banks, in the custody or under the control of each public body; and
- (c) the title, business address and business telephone number of an officer or employee of each public body who may be contacted for information about this Act.

The directory was a hard copy binder that was updated with printed inserts. The abolishment of the directory was intended to be replaced with providing the information on websites. For example, provincial government departments post information about their mandate, functions and organization charts on their websites. The FIPPA website provides contact information for access and privacy coordinators.

However, there does not appear to be any descriptions of records, as described above in clause 75(2)(b), posted on the provincial government website. These descriptions should be posted online or another option may be to post the actual records schedules, which may be more straightforward as these documents already exist. Currently, provincial government records schedules are available to the public by attending the Archives of Manitoba in person.

## **Recommendation 2**

Consideration should be given to amending FIPPA to increase and strengthen proactive disclosure and open government initiatives. Information that describes records held by public bodies, or records schedules, should be posted online.

## **3. ACCESS TO INFORMATION – PROCEDURAL MATTERS**

### **APPLICATION FOR ACCESS FORM**

#### **Issue**

Applicants sometimes mistakenly ask for answers to questions rather than access to records on an application form.

The application for access form needs to have more space for the applicant to clearly indicate their street address or post office box number as well as their city or town.

#### **Discussion**

FIPPA provides a right of access to records. When an applicant simply asks a question on the form, instead of requesting records that may provide answers to their questions, public bodies may need clarification from them which can result in delays in processing the request. The instructions for completing the application form could make clear that the form should not be used to simply ask questions.

The application for access form has separate boxes in which the applicant is to fill in their address, postal code and province. The box on the form for the “Address” is intended to capture both the street address/post office box number as well as the city/town. However, there is not enough space for an applicant to legibly write both and sometimes they only include one part of their address. There should be dedicated spaces for the applicant to fill in their street address/post office box number, and their city/town.

## **Recommendation 3**

On the “Instructions” page of the application form, after an applicant is asked to “Describe the records or information to which you want access to in as much detail as possible,” add a sentence to explain that the form is not to be used for asking questions.

Modify the application for access form to provide dedicated spaces for the applicant to fill in their street address/post office box number and their city/town.

## REQUESTS THAT INVOLVE PERSONAL HEALTH INFORMATION TO WHICH PHIA APPLIES

### Issue

Where an access request is made under FIPPA by an individual seeking a record that contains his or her own personal health information (PHI), the request must be made under PHIA, and Part 2 of FIPPA (Access to Information) does not apply. FIPPA does not address circumstances in which a record contains information to which both FIPPA and PHIA may apply.

### Discussion

Public bodies are also trustees under PHIA with respect to any PHI they hold. Individuals have a right of access to general information and their own personal information (PI) under FIPPA and their PHI under PHIA. An individual may request their own information under FIPPA, however if the “record” contains their PHI, they must make a request under PHIA.

The relevant provision of FIPPA states:

**Part does not apply to individual's personal health information**

**6(1)** An individual seeking access to a record containing his or her own personal health information must request access under *The Personal Health Information Act*, and this Part does not apply.

The above provision appears to require an access request for the entire record to be made under PHIA, despite that the record may contain other information to which PHIA does not apply.

Given that public bodies may hold both PI and PHI of an individual, and an individual may not be aware that two laws apply, the individual may decide to use the FIPPA application form in various circumstances, including:

- where a record or records contain a mixture of both PI and PHI within the same record
- where some records contain PI and other records contain PHI
- when the records contain only PHI

In any of the above circumstances, the individual should not be required to submit a new or additional request for PHI. Under PHIA a request for access may be made verbally or in writing, however there is no prescribed form under PHIA. Accordingly, an application for access under FIPPA could be treated as a written request under PHIA, where PHI is involved.

Alberta’s Freedom of Information and Protection of Privacy Act addresses these issues by requiring a public body to treat a FIPPA request that includes PHI to which their Health Information Act applies, as if it were a request under that act. This provision states:

**Request under section 7 deemed to be a request under HIA**

**15.1(1)** If a request is made under section 7(1) for access to a record that contains information to which the Health Information Act applies, the part of the request that relates to that information is deemed to be a request under section 8(1) of the Health Information Act and that Act applies as if the request had been made under section 8(1) of that Act.

#### **Recommendation 4**

Subsection 6(1) of FIPPA should be amended to require a public body to treat a FIPPA request that includes PHI to which PHIA applies, as if it were a request under that act, similar to subsection 15.1(1) of Alberta's FIPPA.

### **ABANDONED REQUESTS**

#### **Issue**

Further to making a request for access, an individual may decide not to pursue the request for various reasons. FIPPA does not enable a public body to consider a request to be abandoned by an applicant when the applicant does not provide clarification about a request that is necessary in order to process the request.

#### **Discussion**

A public body may consider a request to be abandoned under subsection 82(3) if an applicant does not respond within 30 days about a fee estimate for processing a request by either accepting the fee or modifying the request to change the amount of the fee. However, there could be other circumstances in which requests may be abandoned, such as when a public body needs clarification from an applicant about a request in order to process it and no clarification is received.

A public body may extend the time limit for responding if the applicant does not give enough detail to enable the public body to identify a requested record. Despite that an applicant may abandon a request, a public body may be still obligated to provide a response to the request, as there is no provision in the act to release the public body from the obligation to respond.

The legislation in Alberta, New Brunswick and Prince Edward Island contain similar wording regarding abandoned requests. As an example, below are the relevant provisions from New Brunswick's act:

#### **Application deemed abandoned**

**12(1)** If the head of the public body sends to the applicant a request for clarification in writing or a request in writing that the applicant shall pay or agree to pay fees for access to a record and the applicant does not respond to the request within 30 days after receiving the request, the request for access to a record shall be deemed abandoned.

**12(2)** If the request is deemed abandoned under subsection (1), the head shall notify the applicant in writing of his or her right to file a complaint with the Commissioner with respect to the abandonment.

Alberta's Freedom of Information and Protection of Privacy Act contains the following provisions:

**Abandoned request**

**8(1)** Where the head of a public body contacts an applicant in writing respecting the applicant's request, including

(a) seeking further information from the applicant that is necessary to process the request, or

(b) requesting the applicant to pay a fee or to agree to pay a fee,

and the applicant fails to respond to the head of the public body, as requested by the head, within 30 days after being contacted, the head of the public body may, by notice in writing to the applicant, declare the request abandoned.

**(2)** A notice under subsection (1) must state that the applicant may ask for a review under Part 5.

The above examples provide a reasonable option, which may be exercised by a public body in specified circumstances. It ensures accountability as the public body must contact the applicant in writing to seek further information or payment of a fee before a request can be considered to be abandoned. If the applicant does not respond to the public body within 30 days, the public body may then consider the request to be abandoned.

Additionally, the public body must provide written notice to the applicant about the decision to declare the access request to be abandoned and it is important to include the obligation to inform the individual of the right of complaint to the ombudsman about that decision.

**Recommendation 5**

FIPPA should permit a public body to decide that a request has been abandoned based on specified circumstances, such as when the individual does not provide necessary clarification about their request or accept or pay a fee. The public body should provide notice of this decision in writing to the applicant, explain the reason for the decision, and inform the applicant of the right of complaint about the decision.

**FEES****Issue**

Some public bodies provide applicants with copies of records via CD-ROM, DVD or USB flash drive instead of, or as an option to, providing photocopies of paper records. Given that the actual cost of this storage medium is known up front, the Estimate of Costs form should incorporate this cost, for clarity and efficiency in the payment process between public bodies and applicants.

Also, the FIPPA discussion paper indicated that half of the jurisdictions in Canada have an application fee and invited comments on whether to charge a fee for multiple or concurrent requests.

**Discussion**

Subsection 5(1) of the Access and Privacy Regulation under FIPPA specifies copying fees for records, as follows:

**Copying fees**

**5(1)** An applicant who is given a copy of a record shall pay the following copying fees to the public body:

- (a) 20 cents for each page for paper copies made by a photocopier or computer printer;
- (b) 50 cents for each page for paper copies made from a micro printer,
- (c) actual costs for any other method of providing copies

**5(2)** Despite subsection (1), an applicant requesting copies of his or her own personal information is not required to pay a copying fee if the total copying fee payable is less than \$10.00.

Under clause 5(1)(c) above, a public body may charge the actual costs for any other method of providing copies. Some public bodies provide copies of records via CD-ROM, DVD or USB flash drive instead of, or as an option to, providing photocopies of paper records, and they may charge the actual cost of the storage medium.

When a large number of pages are involved, copying the records to a storage medium may be a less costly way for an applicant to obtain a copy of the records. A public body may also save time copying records to a storage medium rather than making copies on a photocopier.

In providing an Estimate of Costs form to an applicant, whenever a public body estimates that search and preparation time will take more than two (free) hours, it would make sense to include the actual cost for providing a copy on a storage medium. The actual cost of the storage medium is fixed and unlikely to change.

Although a public body may inform the applicant of the cost of the storage medium in a cover letter sent with the Estimate of Costs form, it would be more straightforward to include this actual cost directly on the form to make it clear and ensure the correct payment is made. This would avoid having the applicant send a separate payment for the storage medium at a later date in order to receive the records.

Currently, the Estimate of Costs form does not enable a public body to charge the actual cost for the method of providing a copy on a storage medium, as is allowed under clause 5(1)(c). The form states that it includes charges authorized under sections 4 (search and preparation) and 6 (computer programming and data processing) of the Access and Privacy Regulation. It does state that there is generally an extra charge for obtaining copies.

We note that obtaining payment up front for *estimated costs* for *photocopies* would be problematic given that after receiving the Estimate of Costs, an applicant may modify their request in order to change the amount of the fees, which can reduce the number of copies and the amount payable. Also, an applicant may wish to examine all records to which they are granted access and only obtain copies of some pages. But the *actual* cost of providing a copy on a storage medium is a fixed amount that is known up front.

There should be space on the Estimate of Costs form to include the actual cost of other methods of providing a copy of the records, as set out under clause 5(1)(c), so the total amount for the applicant to pay is clear.

With respect to the issue of potentially charging an application fee, this may be perceived by some citizens as a barrier to access and may dissuade some from making a request. Charging fees for the time spent in processing a request is proportional to the work involved in any given request and may provide an incentive to focus a request on specific records the applicant is seeking.

The discussion paper raised the issue of charging a fee for multiple or concurrent requests. We understand that responding to applicants who make a significant number of requests may have an impact on responding to subsequent requests, for example by citizens who may only have made one request. However, individuals or organizations who can afford to pay application fees may not be deterred from making multiple or concurrent requests. If the issue is really about dealing with high volumes of requests by some individuals or organizations, consideration could be given to addressing that issue in a way that does not impact all applicants.

### **Recommendation 6**

The Estimate of Costs form should be amended to enable a public body to include the actual cost of providing a copy of records, as set out under clause 5(1)(c) of the Access and Privacy Regulation. This would permit public bodies to calculate for the applicant the total fee including the cost of providing a copy on a storage medium, such as a CD-ROM, DVD or USB flash drive.

With respect to the question of implementing an application fee, we are of the view that this may deter the general public from making requests and that it may not address the issue of time or costs in dealing with multiple and concurrent requests from an individual or an organization.

## **FEE WAIVERS**

### **Issue**

FIPPA enables a public body to waive any fees payable for access to information. A public body has discretion to waive all or part of the fee in certain circumstances described in the regulation. The circumstances for waiving a fee should be expanded to include a broader consideration of fairness to an applicant.

### **Discussion**

The Access and Privacy Regulation under FIPPA sets out the following circumstances in which fees may be waived:

#### **Waiver of fees**

- 9(1)** At the applicant's request, the head of a public body may waive all or part of the fees payable under this regulation if the head is satisfied that
- (a) payment would impose an unreasonable financial hardship on the applicant;
  - (b) the request for access relates to the applicant's own personal information and waiving the fees would be reasonable and fair in the circumstances; or
  - (c) the record relates to a matter of public interest concerning public health or safety or the environment.

While this would not prevent a public body from waiving all or part of a fee in other circumstances, there is no obligation for a public body to consider other circumstances not described above. Subsection 9(1) is discretionary, and so a public body may decide not to waive a fee despite that one of the above clauses applies.

A broader basis for waiving a fee should be included in subsection 9(1). For example, this could relate to other situations in which it would be reasonable and fair in the circumstances to waive all or part of a fee, beyond just for personal information. This broader circumstance would enable consideration of various factors, including if there was an unreasonable delay in responding to the request.

As an example, the acts in Alberta and British Columbia include a broader basis to waive fees if “it is fair to excuse payment.” Below is the relevant section of Alberta’s FIPPA (fees for an individual’s personal information fall under a different section of their act):

**Fees**

**93(4)** The head of a public body may excuse the applicant from paying all or part of a fee if, in the opinion of the head,  
 (a) the applicant cannot afford the payment or for any other reason it is fair to excuse payment,  
 or  
 (b) the record relates to a matter of public interest, including the environment or public health or safety.

**Recommendation 7**

The circumstances for waiving a fee should be expanded to include a broader consideration of fairness to an applicant, by adding a provision such as when waiving a fee would be reasonable and fair in the circumstances.

**NOTICE TO AN APPLICANT AND A THIRD PARTY CONSULTED UNDER SECTION 33**

**Issue**

The process for providing notice of an access decision to an applicant and a third party who has been consulted under section 33 could be improved to more adequately protect both the applicant’s and the third party’s right of complaint about the decision.

**Discussion**

When a public body considers giving access to information that might result in an unreasonable invasion of privacy of an individual who is a third party under section 17 or affect the business interests of a third party under section 18, the public body must give written notice to the third party in accordance with section 33. This enables the third party to consent to the disclosure or make representations to the public body about why the information should not be disclosed.

Once a public body has made an access decision, it must provide written notices of the decision to the third party and to the applicant and advise of the right of complaint in the following circumstances:

**Notice of decision**

**34(2)** On reaching a decision under subsection (1), the head of the public body shall give written notice of the decision, including reasons for the decision, to the applicant and the third party.

**Complaint about decision to give access**

**34(4)** If the head of the public body decides to give access to the record or part of the record, the notice under subsection (2) must state that the applicant will be given access unless the third party makes a complaint to the Ombudsman under Part 5 within 21 days after the notice is given.

**Complaint about decision to refuse access**

**34(5)** If the head of the public body decides not to give access to the record or part of the record, the notice under subsection (2) must state that the applicant may make a complaint to the Ombudsman under Part 5 within 21 days after the notice is given.

With respect to a third party's right of complaint when a public body decides to give access to part or all of the records, the public body cannot give access to the records until 21 days after giving notice, to allow for the time period in which the third party may make a complaint. A public body will be notified by our office upon receipt of a third-party complaint, so that the public body is made aware that it cannot proceed to give access after the 21-day time period expires. However, if a public body is not aware of this and does not confirm with our office that no complaint has been made within the 21-day time period, there is a risk that the third party's records are released right after the 21-day time period, prior to our office notifying that a complaint has been received.

One way that this risk could be reduced could be to require the third party to also notify the public body of a complaint to our office, perhaps by providing the public body with a copy of the complaint form that is being submitted to our office.

With respect to the applicant's right of complaint when a public body decides not to give access to part or all of the information, the time period in which to make the complaint is also 21 days after the notice is given. Where access is refused in part, such as when records have some information severed, the applicant would not have the opportunity to see the information to which they have been granted access before deciding whether to make a complaint. This is because the applicant must make the complaint within 21 days and the public body cannot release the information until after 21 days. An applicant may be satisfied with the information once they have an opportunity to see it, but they must complain before they see it.

While a 21-day time limit for the third party to make a complaint is appropriate because this affects the applicant's right of access, it is unclear why a complaint by the applicant must also be made within 21 days.

We note that in other circumstances an applicant has 60 days from being notified of an access decision to make a complaint. If the time limit for the applicant to complain was changed to also be 60 days from being notified of the access decision under subsection 34(2), if records are released after 21 days into that 60 day period, an applicant would still have time to review the records and decide whether to make a complaint.

An access decision could involve records with third-party information of multiple parties and some may not object to disclosure, or it could involve granting access in part and refusing access to other records based on exceptions that do not relate to the third parties. Having 60 days in which to make a complaint would enable an applicant to carefully consider the decision and review any severing of records before determining whether to make a complaint.

### **Recommendation 8**

The complaint process under section 34 should include extra measures to ensure that a third party's personal or business information does not get released to an applicant without confirming that no complaint has been made within the 21-day time limit. The time frame for an applicant to make a complaint about a decision to refuse access should be changed from 21 days to 60 days.

## **4. ACCESS TO INFORMATION – EXCEPTIONS TO ACCESS**

### **PRIVACY OF A THIRD PARTY**

#### **Issue**

FIPPA sets out a mandatory exception that protects the privacy of individuals. It requires access to personal information of a third party be refused if disclosure would be an unreasonable invasion of the third party's privacy. The limits to the exception, contained in subsection 17(4), should be amended to increase consistency with the ability to disclose business contact information under section 44 of FIPPA, and with the protection of privacy of personal health information (PHI) under PHIA. Additionally, consideration should be given to including other types of expenses to be disclosed under clause 17(4)(e).

#### **Discussion**

Under FIPPA an applicant can apply for access to a third party's personal information, including their PHI. A public body is required under clause 17(2)(a) to refuse access to the third party's PHI because this is deemed to be an unreasonable invasion of privacy. Subsection 17(4) sets out circumstances in which the requirement to refuse access under subsection 17(2) no longer applies. One of these circumstances is clause 17(4)(h) which states that it is not an unreasonable invasion of privacy to release information about an individual who has been dead for more than 10 years. This means that if no other exception applies, the PHI could be released to the applicant. There is no requirement for the applicant to have had a close former relationship with the deceased individual.

Public bodies under FIPPA are also trustees under PHIA concerning the PHI they maintain. There is an inconsistency between FIPPA and PHIA with respect to the privacy of the PHI of a deceased individual. PHIA only permits the personal representative of a deceased individual to make a request for access to the deceased's PHI. Also, PHIA only permits a disclosure of the PHI of a deceased individual to be made to a relative of a deceased and this can only be done if such disclosure is believed not to be an unreasonable invasion of deceased individual's privacy.

The inconsistency between FIPPA and PHIA with respect to the circumstances in which PHI of a deceased individual can be disclosed to a requester should be addressed.

We note that the time period in which personal information (including PHI) of a deceased individual may be disclosed under Alberta and British Columbia's FIPPA is 25 years and in New Brunswick it is 20 years. In Newfoundland and Labrador's act, there is no specified time period and a public body must consider whether the length of time the person has been deceased indicates the disclosure is not an unreasonable invasion of the deceased person's personal privacy. Under Ontario's FIPPA the disclosure to a requester is more restrictive in that a public body may only disclose personal information about a deceased individual to the spouse or a close relative of the deceased individual, if in the circumstances, the disclosure is desirable for compassionate reasons.

Another issue with respect to subsection 17(4) is that it does not enable access to personal information of a type routinely disclosed in a business or professional context, including name, position or title, and business contact information. Amendments to FIPPA that came into effect in 2011 permit a public body, under the privacy provisions in Part 3 of FIPPA, to disclose limited personal information of a third party that is routinely disclosed in a business or professional context, as follows:

**Disclosure of personal information**

**44(1)** A public body may disclose personal information only

(x.1) if the personal information is information of a type routinely disclosed in a business or professional context, and the disclosure

- (i) is limited to the individual's name, position name or title, business address, telephone number, facsimile number and e-mail address, and
- (ii) does not reveal other personal information about the individual or personal information about another individual;

Adding business contact information as described above to subsection 17(4) would enable disclosure of this information to an applicant under the access provisions in Part 2 of FIPPA. This would make disclosure of this personal information under the access provisions consistent with disclosure under clause 44(1)(x.1) under the privacy provisions of Part 3 of the act.

With respect to clause 17(4)(e), the disclosure of expenses relates specifically to travel expenses. Consideration should be given to including other types of expenses. This provision is as follows:

**When disclosure not unreasonable**

**17(4)** Despite subsection (2), disclosure of personal information is not an unreasonable invasion of a third party's privacy if

- (e) the information is about the third party's job classification, salary range, benefits, employment responsibilities or travel expenses
- (i) as an officer or employee of a public body,
- (ii) as a minister, or
- (iii) as an elected or appointed member of the governing council or body of a local public body or as a member of the staff of such a council or body;

**Recommendation 9**

The inconsistency between clause 17(4)(h) of FIPPA and PHIA with respect to the circumstances in which PHI of a deceased individual can be disclosed to a requester should be addressed.

Subsection 17(4) should include a provision to disclose to an applicant the business contact information of a third party described in clause 44(1)(x.1).

Consider including other types of expenses to be disclosed under clause 17(4)(e).

## BUSINESS INTERESTS OF A THIRD PARTY

### Issue

The exception for commercial, financial, labour relations, scientific or technical information supplied in confidence to a public body by a third party is too broad and should be explicitly subject to a harms test.

### Discussion

Section 18 is a mandatory exception that excepts from disclosure information that could reasonably be expected to harm the business interests of a third party. Where a provision under section 18 applies, a public body must refuse access, unless one of the limits to the exception described in subsection 18(3) fits the circumstances, or the public interest override in subsection 18(4) applies, as follows:

#### **Disclosure harmful to a third party's business interests**

**18(1)** The head of a public body shall refuse to disclose to an applicant information that would reveal

- (a) a trade secret of a third party;
- (b) commercial, financial, labour relations, scientific or technical information supplied to the public body by a third party, explicitly or implicitly, on a confidential basis and treated consistently as confidential information by the third party; or
- (c) commercial, financial, labour relations, scientific or technical information the disclosure of which could reasonably be expected to
  - (i) harm the competitive position of a third party,
  - (ii) interfere with contractual or other negotiations of a third party,
  - (iii) result in significant financial loss or gain to a third party,
  - (iv) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied, or
  - (v) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

#### **Tax return information**

**18(2)** The head of a public body shall refuse to disclose to an applicant information about a third party that was collected on a tax return or for the purpose of determining tax liability or collecting a tax.

#### **Exceptions**

**18(3)** Subsections (1) and (2) do not apply if

- (a) the third party consents to the disclosure;
- (b) the information is publicly available;
- (c) an enactment of Manitoba or Canada expressly authorizes or requires the disclosure; or
- (d) the information discloses the final results of a product or environmental test conducted by or for the public body, unless the test was done for a fee paid by the third party.

### **Disclosure in the public interest**

**18(4)** Subject to section 33 and the other exceptions in this Act, a head of a public body may disclose a record that contains information described in subsection (1) or (2) if, in the opinion of the head, the private interest of the third party in non-disclosure is clearly outweighed by the public interest in disclosure for the purposes of

- (a) public health or safety or protection of the environment;
- (b) improved competition; or
- (c) government regulation of undesirable trade practices.

Section 18 is relied upon frequently and the statistics in the FIPPA discussion paper indicated that it was the second most relied upon exception in 2015, being used in access decisions concerning 195 applications for access.

We note that clause 18(1)(b) requires a public body to refuse access to commercial, financial, labour relations, scientific or technical information supplied in confidence by, and treated consistently as confidential information by, the third party. This is problematic because the information simply has to be supplied to a public body by a third party and has been kept confidential by the third party. Clause (b) does not explicitly impose a harms test relating to the disclosure of the information as is the case in clause (c). The fact that the third party has supplied information in confidence and has treated its information as confidential is not solely a determinative or reliable factor in establishing harm.

Clause 18(1)(b) presumes that because the information is considered to be confidential, that disclosure will automatically harm the business interests of a third party. This provision should more clearly require justification of harm that would result from revealing confidential information, as is the case with clause 18(1)(c).

In comparison, other access to information laws in Canada contain an explicit harms test for “confidential information” of a third party.

Ontario’s act requires the information to be of a certain type, to be supplied in confidence and for disclosure to cause one of the specified harms:

### **Third party information**

**17(1)** A head shall refuse to disclose a record that reveals a trade secret or scientific, technical, commercial, financial or labour relations information, supplied in confidence implicitly or explicitly, where the disclosure could reasonably be expected to,

- (a) prejudice significantly the competitive position or interfere significantly with the contractual or other negotiations of a person, group of persons, or organization;
- (b) result in similar information no longer being supplied to the institution where it is in the public interest that similar information continue to be so supplied;
- (c) result in undue loss or gain to any person, group, committee or financial institution or agency; or
- (d) reveal information supplied to or the report of a conciliation officer, mediator, labour relations officer or other person appointed to resolve a labour relations dispute.

### **Tax information**

**(2)** A head shall refuse to disclose a record that reveals information that was obtained on a tax return or gathered for the purpose of determining tax liability or collecting a tax.

Newfoundland and Labrador's act contains similar wording to Ontario, however it more clearly sets out a three-part test which includes the type of information, that the information was supplied in confidence and that disclosure of it would cause one of the specified harms:

**Disclosure harmful to business interests of a third party**

- 39. (1)** The head of a public body shall refuse to disclose to an applicant information
- (a) that would reveal
    - (i) trade secrets of a third party, or
    - (ii) commercial, financial, labour relations, scientific or technical information of a third party;
  - (b) that is supplied, implicitly or explicitly, in confidence; and
  - (c) the disclosure of which could reasonably be expected to
    - (i) harm significantly the competitive position or interfere significantly with the negotiating position of the third party,
    - (ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied,
    - (iii) result in undue financial loss or gain to any person, or
    - (iv) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

- (2)** The head of a public body shall refuse to disclose to an applicant information that was obtained on a tax return, gathered for the purpose of determining tax liability or collecting a tax, or royalty information submitted on royalty returns, except where that information is non-identifying aggregate royalty information.

The provisions in the acts in Alberta, Yukon, Nova Scotia and Prince Edward Island contain essentially the same wording as in Newfoundland and Labrador's act.

**Recommendation 10**

Section 18 should be amended to more clearly require a demonstrable harm to a third party's business interests that could reasonably be expected to result from disclosure of confidential information of a third party. Newfoundland and Labrador, Alberta, Yukon, Nova Scotia and Prince Edward Island have wording that should be used a model to clearly impose a three-part test.

**LABOUR RELATIONS INTERESTS OF A PUBLIC BODY AS EMPLOYER**

**Issue**

A public body must refuse access under subclause 18(1)(c)(v) to a *third party's* labour relations information that could reasonably cause harm to the third party, however there is no parallel provision for a *public body's* labour relations information.

## Discussion

Labour relations information of a third party is excepted from disclosure under subclause 18(1)(c)(v). This exception applies to a third party's commercial, financial, labour relations, scientific or technical information, if the disclosure could reasonably be expected to reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute. Section 18 is intended to protect a third party's business interests, not those of a public body. However, there is no corresponding exception regarding labour relations information of public bodies and sometimes public bodies claim subclause 18(1)(c)(v) in error for their own labour relations information.

Section 28 of FIPPA protects the economic and other interests of a public body. Labour relations information is not specifically mentioned in this exception however the listing of types of information is not intended to be exhaustive and a public body can include other types of information that would be harmful to economic or other interests of a public body. Section 28 states:

### **Disclosure harmful to economic and other interests of a public body**

**28(1)** The head of a public body may refuse to disclose information to an applicant if disclosure could reasonably be expected to harm the economic or financial interests or negotiating position of a public body or the Government of Manitoba, including the following information:

- (a) a trade secret of a public body or the Government of Manitoba;
- (b) financial, commercial, scientific, technical or other information in which a public body or the Government of Manitoba has a proprietary interest or right of use;
- (c) information the disclosure of which could reasonably be expected to
  - (i) result in financial loss to,
  - (ii) prejudice the competitive position of, or
  - (iii) interfere with or prejudice contractual or other negotiations of, a public body or the Government of Manitoba;
- (d) innovative scientific or technical information obtained through research by an employee of a public body or the Government of Manitoba; or
- (e) information the disclosure of which could reasonably be expected to result in an undue loss or benefit to a person, or premature disclosure of a pending policy decision, including but not limited to,
  - (i) a contemplated change in taxes or other source of revenue,
  - (ii) a contemplated change in government borrowing,
  - (iii) a contemplated change in the conditions of operation of a financial institution, stock exchange, or commodities exchange, or of any self-regulating association recognized by The Manitoba Securities Commission under an enactment of Manitoba, or
  - (iv) a contemplated sale or purchase of securities, bonds or foreign or Canadian currency.

### **Exception**

**28(2)** Subsection (1) does not apply to the results of a product or environmental test conducted by or for a public body, unless the test was done for the purpose of developing methods of testing or for the purpose of testing products for possible purchase.

Newfoundland and Labrador's act contains a specific exception for labour relations information, as follows:

**Disclosure harmful to labour relations interests of public body as employer**

**38. (1)** The head of a public body may refuse to disclose to an applicant information that would reveal

- (a) labour relations information of the public body as an employer that is prepared or supplied, implicitly or explicitly, in confidence, and is treated consistently as confidential information by the public body as an employer; or
- (b) labour relations information the disclosure of which could reasonably be expected to
  - (i) harm the competitive position of the public body as an employer or interfere with the negotiating position of the public body as an employer,
  - (ii) result in significant financial loss or gain to the public body as an employer, or
  - (iii) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer, staff relations specialist or other person or body appointed to resolve or inquire into a labour relations dispute, including information or records prepared by or for the public body in contemplation of litigation or arbitration or in contemplation of a settlement offer.

**(2)** Subsection (1) does not apply where the information is in a record that is in the custody or control of the Provincial Archives of Newfoundland and Labrador or the archives of a public body and that has been in existence for 50 years or more.

While section 28 of FIPPA could apply to a public body's labour relations information, it would be useful to expressly include an exception for this, either within section 28 or as a stand-alone exception.

**Recommendation 11**

There should be a specific exception for a public body's labour relations information as an employer, either within section 28 or as a stand-alone exception.

**CABINET CONFIDENCES**

**Issue**

To ensure that access decisions are thorough, consent for disclosure as provided for under clause 19(2)(b) should be sought from cabinet when deciding whether to refuse access under section 19. As the process of giving or withholding consent is a discretionary decision that may be exercised by cabinet, section 19 should be a discretionary exception rather than a mandatory one.

The 20-year time period during which a cabinet confidence is protected from disclosure is too long and background information should be disclosed.

**Discussion**

Section 19 is a mandatory exception that requires access to information that would reveal the "substance of deliberations of Cabinet" to be refused. This exception explicitly enables information subject to a cabinet confidence to be disclosed *if* the cabinet for which it was prepared consents to disclosure, under clause 19(2)(b). Accordingly, the requirement to refuse access does not apply if the

cabinet consents to disclosure. The requirement to refuse access also no longer applies to records more than 20 years old as stated in clause 19(2)(b).

The relevant provisions are as follows:

#### **Cabinet confidences**

**19(1)** The head of a public body shall refuse to disclose to an applicant information that would reveal the substance of deliberations of Cabinet, including ....

#### **Exceptions**

**19(2)** Subsection (1) does not apply if

(a) the record is more than 20 years old; or

(b) consent to disclosure is given

(i) in the case of a record prepared for or in respect of the current government, by the Executive Council, and

(ii) in the case of a record prepared for or in respect of a previous government, by the President of the Executive Council of that government or, if he or she is absent or unable to act, by the next senior member of that government's Executive Council who is present and able to act.

Under FIPPA, the duty to assist includes responding to a request openly and completely. Accordingly, consent for disclosure as specifically provided for under clause 19(2)(b) should be sought from cabinet when deciding whether to refuse access under section 19. The consideration of giving or withholding consent is a discretionary decision that may be exercised by cabinet. As there essentially is the ability of cabinet to exercise discretion to consent or not consent to disclose any particular cabinet confidence, section 19 should be a discretionary exception rather than a mandatory one.

We note that under Nova Scotia's act, the exception for cabinet confidences is discretionary, not mandatory. Also, the limits under its clause 13(2)(c) provide transparency of the background information that underpins the decisions of cabinet when disclosure of that information could not reasonably be expected to cause harm. The following is the Nova Scotia exception:

#### **Deliberations of Executive Council**

**13(1)** The head of a public body may refuse to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees, including any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees.

**(2)** Subsection (1) does not apply to

(a) information in a record that has been in existence for ten or more years;

(b) information in a record of a decision made by the Executive Council or any of its committees on an appeal pursuant to an Act; or

(c) background information in a record the purpose of which is to present explanations or analysis to the Executive Council or any of its committees for its consideration in making a decision if

(i) the decision has been made public,

(ii) the decision has been implemented, or

(iii) five or more years have passed since the decision was made or considered.

Although under Alberta's act the exception is mandatory, it contains wording about background information similar to that in Nova Scotia:

**Cabinet and Treasury Board confidences**

**22(1)** The head of a public body must refuse to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees or of the Treasury Board or any of its committees, including any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees or to the Treasury Board or any of its committees.

**(2)** Subsection (1) does not apply to

- (a) information in a record that has been in existence for 15 years or more,
- (b) information in a record of a decision made by the Executive Council or any of its committees on an appeal under an Act, or
- (c) information in a record the purpose of which is to present background facts to the Executive Council or any of its committees or to the Treasury Board or any of its committees for consideration in making a decision if
  - (i) the decision has been made public,
  - (ii) the decision has been implemented, or
  - (iii) 5 years or more have passed since the decision was made or considered.

Subsection 19(2) of FIPPA should enable background information to be disclosed if the decision has been made public, or has been implemented, or five or more years have passed since the decision was made or considered.

We also note that Newfoundland and Labrador's act permits disclosure of a cabinet confidence based on public interest, under subsection 27(3) as follows:

- (3) Notwithstanding subsection (2), the Clerk of the Executive Council may disclose a cabinet record or information that would reveal the substance of deliberations of Cabinet where the Clerk is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception.

The above provision should be added to subsection 19(2) as another basis for which a cabinet confidence may be disclosed.

The cabinet confidence exception continues to protect records for 20 years after the creation of the records. This time frame should be reduced. Several acts in Canada limit the application of the cabinet confidence exception to a time frame lower than 20 years. For example, the time frame is 15 years in British Columbia, Alberta, Yukon, Northwest Territories and Nunavut. The time frame in Nova Scotia is 10 years. In 2016, the Saskatchewan Information and Privacy Commissioner recommended the time frame be reduced from 25 years to 15 years.

**Recommendation 12**

Section 19, Cabinet Confidences, should be changed from a mandatory to a discretionary exception.

Subsection 19(2) should include a new provision to enable background information to be disclosed if the decision has been made public, or has been implemented, or five or more years have passed since the decision was made or considered.

Subsection 19(2) should include a new provision to permit disclosure by the clerk of the executive council where the clerk is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception.

The time frame specified in clause 19(2)(a) after which the exception for cabinet confidences no longer applies should be reduced from 20 years to 15 years or less.

## ADVICE TO A PUBLIC BODY

### Issue

Section 23, advice to a public body, is too broad.

### Discussion

Section 23 sets out exceptions to disclosure with the intent to protect the free flow of advice in a decision-making process involving a public body or a minister. The FIPPA discussion paper indicated that section 23 was the third most frequently used exception in 2015, and was used in access decisions concerning 53 applications. We note that from 2011 to 2014, it was the second most commonly used exception.

Although section 23 is intended to protect advice connected to decision making, the broad wording of this exception can capture non-advice. Clause 23(1)(b) should not capture consultations and deliberations that do not reveal advice that would already be subject to clause 23(1)(a).

Also, the limits contained in subsection 23(2) should be revised. The time limit in clause 23(2)(a) should be reduced. Also, the types of information described as “background research” in clause 23(2)(f) should be expanded.

Section 23 states:

#### **Advice to a public body**

**23(1)** The head of a public body may refuse to disclose information to an applicant if disclosure could reasonably be expected to reveal

(a) advice, opinions, proposals, recommendations, analyses or policy options developed by or for the public body or a minister;

(b) consultations or deliberations involving officers or employees of the public body or a minister;

(c) positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations by or on behalf of the Government of Manitoba or the public body, or considerations that relate to those negotiations;

(d) plans relating to the management of personnel or the administration of the public body that have not yet been implemented;

- (e) the content of draft legislation, regulations, and orders of ministers or the Lieutenant Governor in Council; or
- (f) information, including the proposed plans, policies or projects of a public body, the disclosure of which could reasonably be expected to result in disclosure of a pending policy or budgetary decision.

### **Exceptions**

**23(2)** Subsection (1) does not apply if the information

- (a) is in a record that is more than 20 years old;
- (b) is an instruction or guideline issued to officers or employees of the public body;
- (c) is a substantive rule or statement of policy that has been adopted by the public body for the purpose of interpreting an enactment or administering a service, program or activity of the public body;
- (d) is the result of a product or environmental test conducted by or for the public body;
- (e) is a statement of the reasons for a decision made in the exercise of a quasi-judicial function or a discretionary power that affects the applicant;
- (f) is the result of background research of a scientific or technical nature undertaken in connection with the formulation of a policy proposal;
- (f.1) is a public opinion poll;
- (g) is a statistical survey; or
- (h) is a final report or final audit on the performance or efficiency of the public body or of any of its programs or policies, except where the information is a report or appraisal of the performance of an individual who is or was an officer or employee of the public body.

### **Interpretation of "background research"**

**23(3)** For the purpose of clause (2)(f), background research of a technical nature does not include economic or financial research undertaken in connection with the formulation of a tax policy or other economic policy of the public body.

Under the Freedom of Information Act that was repealed when FIPPA came into effect, the exception for policy opinions, advice or recommendations was narrower and required a connection to the formulation of policy, making of a decision or development of a negotiating position, as follows:

#### **Policy opinions, advice or recommendations.**

**39(1)** Subject to subsection (4), the head of a department may refuse to give access to any record which discloses

- (a) an opinion, advice or a recommendation submitted by an officer or employee of a department, or a member of the staff of a minister, to a department or to a minister for consideration in
  - (i) the formulation of a policy, or
  - (ii) the making of a decision, or
  - (iii) the development of a negotiating position of or by the department or the government; or
- (b) a plan relating to the administration of a department, including a plan relating to the management of personnel, which has not yet been implemented;
- (c) the contents of any draft enactment.

Nova Scotia's act specifically states that background information cannot be withheld under this exception, nor can information that has been in existence for five or more years, as follows:

**Advice to public body or minister**

**14 (1)** The head of a public body may refuse to disclose to an applicant information that would reveal advice, recommendations or draft regulations developed by or for a public body or a minister.

**(2)** The head of a public body shall not refuse pursuant to subsection (1) to disclose background information used by the public body.

**(3)** Subsection (1) does not apply to information in a record that has been in existence for five or more years.

**(4)** Nothing in this Section requires the disclosure of information that the head of the public body may refuse to disclose pursuant to Section 13.\*

\*section 13 refers to the exception for cabinet confidences

Under Newfoundland and Labrador's act, "factual material" cannot be withheld (despite that it could reveal policy advice or recommendations), information that has been publicly cited as the basis for a public body's decision cannot be withheld, nor can information that has been in existence for 15 or more years:

**Policy advice or recommendations**

**29. (1)** The head of a public body may refuse to disclose to an applicant information that would reveal

- (a) advice, proposals, recommendations, analyses or policy options developed by or for a public body or minister;
- (b) the contents of a formal research report or audit report that in the opinion of the head of the public body is incomplete and in respect of which a request or order for completion has been made by the head within 65 business days of delivery of the report; or
- (c) draft legislation or regulations.

**(2)** The head of a public body shall not refuse to disclose under subsection (1)

- (a) factual material;
- (b) a public opinion poll;
- (c) a statistical survey;
- (d) an appraisal;
- (e) an environmental impact statement or similar information;
- (f) a final report or final audit on the performance or efficiency of a public body or on any of its programs or policies;
- (g) a consumer test report or a report of a test carried out on a product to test equipment of the public body;
- (h) a feasibility or technical study, including a cost estimate, relating to a policy or project of the public body;
- (i) a report on the results of field research undertaken before a policy proposal is formulated;
- (j) a report of an external task force, committee, council or similar body that has been established to consider a matter and make a report or recommendations to a public body;
- (k) a plan or proposal to establish a new program or to change a program, if the plan or proposal has been approved or rejected by the head of the public body;

(l) information that the head of the public body has cited publicly as the basis for making a decision or formulating a policy; or

(m) a decision, including reasons, that is made in the exercise of a discretionary power or an adjudicative function and that affects the rights of the applicant.

**(3)** Subsection (1) does not apply to information in a record that has been in existence for 15 years or more.

### **Recommendation 13**

Clause 23(1)(b) that applies to consultations and deliberations should be deleted because any such communications that reveal advice would be subject to 23(1)(a), and if advice is not revealed these communications should not be excepted from disclosure as this is contradictory to the intent of this exception.

Subsection 23(2) should provide for the disclosure of:

- factual material or background information, that is beyond what is currently provided for under subsection 23(2)(f)
- information that has been publicly cited as the basis for a public body's decision
- information that has been in existence for 15 or more years, reduced from 20 years under clause 23(2)(a).

## **INFORMATION THAT WILL BE MADE AVAILABLE TO THE PUBLIC**

### **Issue**

FIPPA permits a public body to refuse access to information that will be made available to the public within 90 days after the applicant's request is received. This time frame should be shortened in view of the shift toward making information available to the public via websites.

### **Discussion**

Section 32 of FIPPA permits access to be refused if a public body intends to publish the information within 90 days of receiving the request. If the information is not made available to the public in that time frame, the request must be treated as a new request received on the 90<sup>th</sup> day and a public body then has up to 30 days to issue a new access decision. An applicant may need to wait for up to 120 days for an access decision. The relevant provisions are as follows:

#### **Information that will be available to the public**

**32(1)** The head of a public body may refuse to disclose to an applicant information that will be made available to the public within 90 days after the applicant's request is received.

#### **Notification when information becomes available**

**32(2)** When the head of a public body has refused to disclose information under subsection (1), the head shall

- (a) notify the applicant when the information becomes available; and

(b) if the information is not available to the public within 90 days after the applicant's request is received, reconsider the request as if it were a new request received on the last day of the 90 day period and not refuse access to the information under subsection (1).

FIPPA came into effect in 1998 when publication generally involved producing printed copies of documents in order to make them available to the public. Increasingly, public bodies are publishing information on websites, which can provide greater control over the publication process and timing and should reduce the amount of time required for publication.

In some jurisdictions, the time frame for this exception is shorter. For example, in British Columbia and Alberta the time frame is 60 days from receipt of the request. In Newfoundland and Labrador this time frame is 30 business days.

#### **Recommendation 14**

The time frame in section 32 should be reduced so that a public body may refuse access to information that will be made available to the public within 60 days, instead of 90 days.

### **PUBLIC INTEREST OVERRIDE FOR EXCEPTIONS**

#### **Issue**

FIPPA should include a public interest override for some exceptions to enable information to be released when the public interest clearly outweighs the reason for the exception.

#### **Discussion**

A public interest override permits disclosure of information that would be subject to an exception and not usually disclosed, to be disclosed when there is an overriding public interest.

FIPPA does not have a public interest override that would enable a disclosure of excepted information to be made when the public interest clearly outweighs the reason for the exception. There is, however, a limited, discretionary override in section 18 for information that would harm a third party's business interests, if the private interest of the third party in non-disclosure is clearly outweighed by the public interest in disclosure for the purposes of public health or safety or protection of the environment, improved competition, or government regulation of undesirable trade practices.

Many access to information laws in Canada do provide a more broadly applicable public interest override and some acts require information to be publicly disclosed in the absence of an application for access being made.

Newfoundland and Labrador's act set out the following public interest override for the specified exceptions listed below:

#### **Public interest**

**9. (1)** Where the head of a public body may refuse to disclose information to an applicant under a provision listed in subsection (2), that discretionary exception shall not apply where it is clearly

demonstrated that the public interest in disclosure of the information outweighs the reason for the exception.

**(2)** Subsection (1) applies to the following sections:

- (a) section 28 (local public body confidences);
- (b) section 29 (policy advice or recommendations);
- (c) subsection 30 (1) (legal advice);
- (d) section 32 (confidential evaluations);
- (e) section 34 (disclosure harmful to intergovernmental relations or negotiations);
- (f) section 35 (disclosure harmful to the financial or economic interests of a public body);
- (g) section 36 (disclosure harmful to conservation); and
- (h) section 38 (disclosure harmful to labour relations interests of public body as employer).

### **Recommendation 15**

FIPPA should contain a public interest override to permit disclosure of information subject to discretionary exceptions to be disclosed when it is clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception. The public interest override in the recently amended act in Newfoundland and Labrador could serve as a useful model.

## **5. PROTECTION OF PRIVACY**

### **PROTECTION OF PERSONAL INFORMATION**

#### **Issue**

The requirements for the protection of personal information (PI) need to be strengthened.

#### **Discussion**

Public bodies hold personal information and personal health information about individuals in order to deliver programs, services or benefits. The requirements for protecting PI under FIPPA are less clear than those for protecting PHI under PHIA, despite that PI can also be very sensitive.

Since the previous review of FIPPA in 2004, many changes have occurred to the ways in which PI is handled by public bodies. Increasingly, PI is being collected, used, disclosed, stored electronically. The requirements for the protection of PI need to be updated and strengthened.

FIPPA requires a public body to protect PI by making “reasonable security arrangements” against risks, as follows:

#### **Protection of personal information**

**41** The head of a public body shall, in accordance with any requirements set out in the regulations, protect personal information by making reasonable security arrangements against such risks as unauthorized access, use, disclosure or destruction.

Public bodies are also trustees under PHIA for any PHI they maintain. In comparison, PHIA contains more robust requirements concerning PHI:

**Duty to adopt security safeguards**

**18(1)** In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.

**Specific safeguards**

**18(2)** Without limiting subsection (1), a trustee shall

- (a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so;
- (b) implement controls to ensure that personal health information maintained by the trustee cannot be used unless
  - (i) the identity of the person seeking to use the information is verified as a person the trustee has authorized to use it, and
  - (ii) the proposed use is verified as being authorized under this Act;
- (c) if the trustee uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the information by unauthorized persons; and
- (d) when responding to requests for disclosure of personal health information, ensure that the request contains sufficient detail to uniquely identify the individual the information is about.

**Additional safeguards for information in electronic form**

**18(3)** A trustee who maintains personal health information in electronic form shall implement any additional safeguards for such information required by the regulations.

**Safeguards for sensitive information**

**19** In determining the reasonableness of security safeguards required under section 18, a trustee shall take into account the degree of sensitivity of the personal health information to be protected.

The Personal Health Information Regulation under PHIA also contains requirements relating to the protection of PHI, including but not limited to the following:

**Written security policy and procedures**

**2** A trustee shall establish and comply with a written policy and procedures containing the following:

- (a) provisions for the security of personal health information during its collection, use, disclosure, storage, and destruction, including measures
  - (i) to ensure the security of the personal health information when a record of the information is removed from a secure designated area, and
  - (ii) to ensure the security of personal health information in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose;

- (b) provisions for the recording of security breaches;
- (c) corrective procedures to address security breaches.

### **Access restrictions and other precautions**

**3** A trustee shall

- (a) ensure that personal health information is maintained in a designated area or areas and is subject to appropriate security safeguards;
- (b) limit physical access to designated areas containing personal health information to authorized persons;
- (c) take reasonable precautions to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction or loss and other hazards; and
- (d) ensure that removable media used to record personal health information is stored securely when not in use.

### **Recommendation 16**

The requirements for the protection of personal information need to be updated and strengthened. PHIA should serve as a model for strengthening the requirements in FIPPA.

## **MANDATORY PRIVACY BREACH NOTIFICATION**

### **Issue**

FIPPA does not require public bodies to notify an individual or the ombudsman when the individual's PI is stolen, lost, used or disclosed without authority, despite that such breaches may result in significant harm to individuals.

### **Discussion**

Providing notification to affected individuals enables them to take steps to reduce the risks to themselves arising from the breach. Significant harm may include physical harm, humiliation, damage to reputation or relationships, financial loss, identity theft, as well as loss of employment or business opportunities. Our practice note, [Key Steps in Responding to Privacy Breaches](#), contains guidance on the types of information to be included in a notice to an individual.

Notification to the ombudsman can help to ensure that a public body takes appropriate steps to address the breach and prevent future breaches. While a small number of privacy breaches are voluntarily reported to the ombudsman, a requirement to report breaches where there may be a significant risk of harm to individuals would make such reporting more consistent and it would enable our office to monitor the public body's response to the breach and provide advice.

All public bodies under FIPPA are also trustees under PHIA for any PHI they maintain. The PHIA discussion paper noted that several health information laws in Canada either have requirements to provide notification to individuals and information and privacy commissioners, or have proposed such requirements. We have recommended that PHIA should also include requirements to notify individuals and the ombudsman of privacy breaches where a trustee reasonably believes that the breach may result in a real risk of significant harm.

With respect to FIPPA laws, we note that the law in Newfoundland and Labrador contains requirements concerning notification of breaches. Information and privacy commissioners in British Columbia, Alberta and Saskatchewan have also suggested that mandatory notification be included in their FIPPA laws.

### **Recommendation 17**

FIPPA should include requirements to notify individuals and the ombudsman of a privacy breach where a public body reasonably believes that the breach may result in a real risk of significant harm to the individual. Prescribing the types of information to include in notification to individuals may ensure adequate notice is given as a matter of accountability by the public body and fairness to the individual, and it may assist the individual to take any steps necessary to assess and address their own risks.

## **SECURE DESTRUCTION OF PERSONAL INFORMATION**

### **Issue**

FIPPA does not set out a requirement concerning the secure destruction of personal information.

### **Discussion**

Personal information may be contained in various formats, including different types of paper records and electronic information stored on or captured by computers, laptops, smartphones, storage mediums, fax machines, printers and copiers. Careful consideration should be given to the method of destruction of the PI, to ensure it is destroyed in a manner that protects privacy.

PHIA expressly requires that the method of destruction must protect privacy, as follows:

#### **Method of destruction must protect privacy**

**17(3)** In accordance with any requirements of the regulations, a trustee shall ensure that personal health information is destroyed in a manner that protects the privacy of the individual the information is about.

### **Recommendation 18**

FIPPA should include a requirement to ensure that personal information is destroyed in manner that protects the privacy of the individual the information is about, as is required for personal health information subject to PHIA.

## **CORRECTION OF PERSONAL INFORMATION**

### **Issue**

Under FIPPA, individuals have a right to request a correction to their PI obtained through an access request if they believe there is an error or omission in the information. There is no requirement for a public body to inform the individual of its decision *in writing* when the public body makes the requested correction or refuses to correct the record.

If a public body refuses to make a requested correction, it must add the individual's request for correction to the record. FIPPA should allow an individual to file a concise statement of disagreement that must be added to the record, as is the case under PHIA concerning a refusal to correct PHI.

## **Discussion**

An individual's request for correction must be in writing. However, a public body's decision about that request is not required to be given in writing, even when the public body refuses to correct the record. The following are the relevant provisions in FIPPA:

### **Right to request correction**

**39(1)** An applicant who has been given access to a record containing his or her personal information under Part 2 and who believes there is an error or omission in the information may request the head of the public body that has the information in its custody or under its control to correct the information.

### **Written request**

**39(2)** A request must be in writing.

### **Head's response**

**39(3)** Within 30 days after receiving a request under subsection (1), the head of the public body shall

- (a) make the requested correction and notify the applicant of the correction; or
- (b) notify the applicant of the head's refusal to correct the record and the reason for the refusal, that the request for correction has been added to the record, and that the individual has a right to make a complaint about the refusal under Part 5.

When a public body refuses to make a correction, it must add the individual's request for correction to the record. We note that PHIA allows an additional step by the individual by permitting the individual to file a concise statement of disagreement, as follows:

### **When a trustee refuses to make a correction**

**12(4)** A trustee who refuses to make a correction that is requested under this section shall

- (a) permit the individual to file a concise statement of disagreement stating the correction requested and the reason for the correction; and
- (b) add the statement of disagreement to the record in such a manner that it will be read with and form part of the record or be adequately cross-referenced to it.

An individual should have an opportunity to explain why they disagree with the public body's refusal to correct the record, by filing a concise statement of disagreement after being notified of a refusal.

## **Recommendation 19**

A public body's response to an individual's request for correction should be required to be in writing. An individual should be permitted to file a concise statement of disagreement about a public body's decision to refuse to correct the record.

## NO ADVERSE EMPLOYMENT ACTION

### Issue

The PHIA discussion paper raised the issue of preventing reprisal by all trustees against employees who (proactively) disclose contraventions of PHIA to the ombudsman. The current protection under PHIA and FIPPA is the same and relates to employees of public bodies and trustees who disclose in *response* to a request for information from the ombudsman.

### Discussion

FIPPA prohibits a public body from taking “adverse employment action” against an employee who complied with the ombudsman’s request to provide information, as follows:

#### **No adverse employment action**

**86(2)** A public body or a person acting on behalf of a public body shall not take any adverse employment action against an employee because the employee has complied with a request or requirement to produce a record or provide information or evidence to the Ombudsman or the adjudicator, or a person acting for or under the direction of the Ombudsman or the adjudicator, under this Act.

This provision relates to *responding* to the ombudsman and does not refer to situations where an employee may believe that it is important to *proactively* disclose suspected or known contraventions to the ombudsman. In our submission about PHIA, we commented about non-retaliation provisions in other health information laws that relate to broader circumstances, including proactively disclosing a contravention and protecting employees from various types of retaliatory behaviour.

We also note that employees of public bodies have a right of complaint to the ombudsman about access requests made to, or about the handling of their PI by, the employer. No adverse employment action should be taken against an employee who chooses to exercise their rights under FIPPA.

Manitoba’s Public Interest Disclosure (Whistleblower Protection) Act (PIDA) provides a process for reporting a “wrongdoing” in the public service. A wrongdoing as defined under PIDA includes an act that is an offence under another law, which includes offences under PHIA. PIDA may not apply to all matters under FIPPA that are contraventions of FIPPA but not “offences.”

The PHIA discussion paper noted that the Saskatchewan information and privacy commissioner recently recommended that province’s health information law be amended to include protection for employees who disclose contraventions of their health information law. This was based on provisions found in other provinces. Newfoundland and Labrador’s PHIA, British Columbia’s FIPPA, the federal Personal Information Protection and Electronic Documents Act all contain similar wording regarding non-retaliation. Below is the relevant section from Newfoundland and Labrador’s PHIA:

#### **Non-retaliation**

**89.** A person shall not dismiss, suspend, discipline, demote, harass or otherwise disadvantage or penalize an individual where

- (a) the individual, acting in good faith and on the basis of reasonable belief, has disclosed to the commissioner that another person has contravened or is about to contravene a provision of this Act or the regulations;
- (b) the individual, acting in good faith and on the basis of reasonable belief has done or stated an intention of doing an act that is required to be done in order to avoid having a person contravene a provision of this Act or the regulations;
- (c) the individual, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention to refuse to do an act that is in contravention of this Act or the regulations; or
- (d) another person believes that the individual will do an act described in paragraph (a), (b) or (c).

### **Recommendation 20**

Subsection 86(2) of FIPPA should not limit the protection for employees to situations in which the disclosure has been made at the request of the ombudsman. Also, no adverse employment action should be taken against employees who exercise their right to make a FIPPA complaint to the ombudsman about their employer. Consideration should be given to whether the phrase “adverse employment action” should be more clearly set out by including the actions described in Newfoundland and Labrador’s PHIA.

## **BIG DATA ANALYTICS**

### **Issue**

The FIPPA and PHIA discussion papers included the issue of using de-identified information to perform data analytics for the purpose of improving services to Manitobans. Big data analytics (BDA) involves the use of technology to analyze large and varied sets of data to uncover hidden patterns, unknown correlations or trends that can be used to inform government policy development and decisions about service delivery. We commented on this issue in our PHIA submission. As government holds both PI and PHI, the same considerations would be applicable to FIPPA.

### **Discussion**

We note that the PHIA discussion paper indicated that BDA in health and social sectors involves two basic enablers, as follows:

- de-identification alters data to remove or obscure personal identifiers and personal information
- data linking joins separate datasets for a more complete view of previously separated information

There is a risk that if de-identification is not done effectively, that the linking of various sets of de-identified data may make the data identifiable and result in the identification of individuals.

The PHIA discussion paper noted that the Manitoba Centre for Health Policy (MCHP) at the University of Manitoba maintains a repository of de-identified data that is used for approved research purposes. The repository was developed to describe and explain patterns of health care and profiles of health and illness, through research in areas such as health care, education and social services. This de-identified

data comes from a variety of government departments. Identifiers, such as names and addresses, are removed before the data is transferred to the repository. Each record comes with a scrambled identifier, which enables various de-identified records about a person to be linked together for specific research processes, without knowing who the person is.

There are well-established processes in place in the provincial government to de-identify PI and PHI and transfer the de-identified data to the repository. MCHP has strict security and protocols in place to manage the de-identified data in the repository, which is treated in the same manner as if it were identifiable PI and PHI. These factors would support data analytics to be performed by the provincial government using the de-identified data in the repository at the MCHP. As the intent of big data analytics is to inform decisions about government policy and delivery of services to the public, transparency about the use of BDA and about the findings or results of conducting BDA would contribute to public trust in the use of their data for this purpose.

### **Recommendation 21**

The de-identification processes used by the provincial government to provide information to the repository of de-identified datasets at the Manitoba Centre for Health Policy would support an increased use of big data analytics by the provincial government. If amendments to FIPPA are necessary to enable this, the risks of re-identifying individuals through the linkage of multiple datasets requires that these processes are carefully managed.

## **6. OVERSIGHT ROLE OF THE OMBUDSMAN**

### **RENAME TITLE TO INFORMATION AND PRIVACY COMMISSIONER**

#### **Issue**

It is generally understood that access and privacy laws are overseen by an information and privacy commissioner, the title which is associated with such laws. The use of the title of ombudsman when performing duties of an information and privacy commissioner under FIPPA and PHIA may contribute to a perception that Manitobans do not have an information and privacy commissioner.

#### **Discussion**

In Manitoba, access to information and privacy rights under PHIA and FIPPA are overseen by the ombudsman appointed under the Ombudsman Act. However, the nature of the ombudsman's role and responsibilities under FIPPA and PHIA are not reflected in the title of the person with such oversight. Manitobans also have information access and privacy rights under federal laws, which are overseen federally by an information commissioner and a privacy commissioner.

In every jurisdiction in Canada, except Manitoba, access to information and privacy legislation is overseen by a person called an information and privacy commissioner (the Nova Scotia legislation refers to the person as the review officer, however, the title of that person has been changed to information and privacy commissioner). Most commissioners have the power to make recommendations, not

orders, as is the case in Manitoba. Manitoba's FIPPA and PHIA should be amended to use the term information and privacy commissioner.

In Yukon, where the ombudsman also serves as the information and privacy commissioner, the access and privacy legislation refers to the person in this role as the information and privacy commissioner. The Yukon access and privacy legislation states that the ombudsman appointed under the Ombudsman Act is the information and privacy commissioner under their FIPPA and PHIA equivalent laws. Section 40 of the Access to Information and Protection of Privacy Act (ATIPPA) states that "commissioner" means the information and privacy commissioner appointed under section 40." Yukon's health information law references this by stating that "commissioner" under their health information law means the information and privacy commissioner appointed under ATIPPA.

An additional point to consider is that in Manitoba, the ombudsman has three distinct mandates under four different laws, the Ombudsman Act, the Public Interest Disclosure (Whistleblower Protection) Act as well as serving as the information and privacy commissioner for Manitoba under FIPPA and PHIA. The legislation setting out the mandates of other independent offices of the Legislative Assembly of Manitoba specifically enable the ability to appoint a deputy (deputy chief electoral officer, deputy auditor general, deputy children's advocate—under the proposed act). As well, section 58.3(1) of FIPPA sets out the ability to appoint a deputy information and privacy adjudicator to assist the adjudicator in reviewing matters referred by the ombudsman when recommendations made under FIPPA and PHIA have not been followed. Given the scope of the ombudsman's mandates under FIPPA and PHIA, and the proactive powers and duties in addition to investigations, these acts should specifically provide for the ombudsman to appoint a deputy information and privacy commissioner under FIPPA and PHIA. Although nothing prohibits having a deputy position, specifying it in FIPPA and PHIA would be consistent with legislation setting out the mandates of other independent officers.

## **Recommendation 22**

FIPPA and PHIA should be amended to change the ombudsman's title under these acts to information and privacy commissioner and the legislation in Yukon could serve as a model. The acts should also be amended to specifically enable the appointment of a deputy information and privacy commissioner.

## **POWERS OF THE OMBUDSMAN CONCERNING AUDITS**

### **Issue**

In addition to the investigation of complaints, the ombudsman has other responsibilities under FIPPA, including the power and duty under clause 49(a) to conduct investigations and audits and make recommendations to monitor and ensure compliance with the act. The provisions which enable the ombudsman to obtain information necessary to perform these duties refer only to investigations and do not specifically include audits.

### **Discussion**

It is necessary for the ombudsman to be able to obtain or examine all relevant records regardless of whether the duty being performed is an investigation or an audit. Subsection 50(2), which enables the ombudsman to require records maintained by a public body to be produced to the ombudsman, does not include being able to do so in relation to conducting an audit. However, the ombudsman's right

under section 51 to enter a public body's office relates more broadly to "exercising powers or performing duties" under the act. These provisions are as follows:

**Production of records**

**50(2)** The Ombudsman may require any record in the custody or under the control of a public body that the Ombudsman considers relevant to an investigation to be produced to the Ombudsman and may examine any information in a record, including personal information.

**Right of entry**

**51** Despite any other enactment or any privilege of the law of evidence, in exercising powers or performing duties under this Act, the Ombudsman has the right

- (a) to enter any office of a public body and examine and make copies of any record in the custody of the public body; and
- (b) to converse in private with any officer or employee of a public body.

Additionally, it should be clarified that the information that public bodies provide during an audit has the same protection under FIPPA as that which is obtained by the ombudsman during an investigation. The following provisions refer to investigations but do not specifically include audits:

**Statements and reports not admissible in evidence**

**53(1)** A statement made or an answer given by a person during an investigation by the Ombudsman, and a report or recommendation of the Ombudsman, is inadmissible in evidence in a court or in any other proceeding, except

- (a) in a prosecution for perjury in respect of sworn testimony;
- (b) in a prosecution for an offence under this Act;
- (c) in a review conducted by the adjudicator under this Act when the Ombudsman is a party;
- or
- (d) in an application for judicial review of an adjudicator's order under this Act.

**Privilege**

**54** Anything said, any information supplied, and any record produced by a person during an investigation by the Ombudsman under this Act is privileged in the same manner as if it were said, supplied or produced in a proceeding in a court.

**Recommendation 23**

The provision that enables the ombudsman to require records maintained by a public body to be produced to the ombudsman should be amended to include being able to do so in relation to conducting an audit. The provisions that provide protection for records produced to the ombudsman during an investigation should also include audits.

**PRODUCTION OF RECORDS OVER WHICH SOLICITOR-CLIENT PRIVILEGE IS CLAIMED**

**Issue**

FIPPA does not expressly enable the ombudsman to require a public body to produce records over which the exception for solicitor-client privilege has been claimed by a public body to refuse access to an

applicant. Where it is necessary to review such records in order to verify a claim, the ombudsman may not be able to conduct an investigation as required by FIPPA.

## Discussion

FIPPA provides an independent and informal review of access decisions of public bodies by the ombudsman. This includes decisions where access has been refused, in which case it is generally necessary for the ombudsman to be able to review the withheld records to determine whether or to what extent the claimed exceptions apply.

It had been understood that the power to review relevant records, despite “any privilege of the law of evidence” included records to which a public body has refused access on the basis of the exception for solicitor-client privilege. For several years, it was accepted that the ombudsman had the power to review any record to which access had been refused, to be able to independently review and determine whether the claimed exceptions apply. However, legal challenges to this power have occurred in other jurisdictions across Canada with similarly worded provisions. These court cases have been cited by Manitoba public bodies who refuse to allow the ombudsman to review records to investigate a claim of solicitor-client privilege as a basis to refuse access.

Access to information laws across Canada have similarly worded provisions for producing records required in an investigation. This issue has been the subject of court cases in other jurisdictions, most notably in Alberta, in a refusal of access case which went through the courts of Alberta and to the Supreme Court of Canada, in Newfoundland and Labrador, and most recently in Saskatchewan. We believe that it is necessary to change the wording in Manitoba’s FIPPA to avoid costly court intervention over disputes relating to what we understand the intent of the legislature to be.

At issue is that the phrase in sections 50 and 51 of FIPPA, “despite any other enactment or any privilege of the law of evidence” does not expressly include solicitor-client privilege:

### **Evidence Act powers**

**50(1)** The Ombudsman has all the powers and protections of a commissioner under Part V of *The Manitoba Evidence Act* when conducting an investigation under this Act.

### **Production of records**

**50(2)** The Ombudsman may require any record in the custody or under the control of a public body that the Ombudsman considers relevant to an investigation to be produced to the Ombudsman and may examine any information in a record, including personal information.

### **Records to be produced within 14 days**

**50(3)** A public body shall produce to the Ombudsman within 14 days any record or a copy of a record required under this section, despite any other enactment or any privilege of the law of evidence.

### **Examination of record on site**

**50(4)** If a public body is required to produce a record under this section and it is not practicable to make a copy of it, the head of the public body may require the Ombudsman to examine the original at its site.

**Right of entry**

- 51** Despite any other enactment or any privilege of the law of evidence, in exercising powers or performing duties under this Act, the Ombudsman has the right
- (a) to enter any office of a public body and examine and make copies of any record in the custody of the public body; and
  - (b) to converse in private with any officer or employee of a public body.

In recent years, our office has adopted practices for dealing with complaints where access has been refused on the basis of the exception for solicitor-client privilege, to minimize the intrusion into such privilege. Sometimes, the nature of information requested along with comprehensive written representations from the public body can establish whether or not the exception applies. However, in some cases that is not sufficient to determine whether the exception applies. If a public body refuses to make the records available to our office because of the wording of sections 50 and 51, our office may be unable to complete the investigation and make a finding on whether or not the exception applies.

In April 2017, the information and privacy commissioner of Alberta submitted a special report to the Alberta Legislative Assembly on this issue. The commissioner noted that the Supreme Court of Canada had said that the Alberta legislature “did not use the right words” in the Alberta act and that the operation of the act and her ability to perform the functions as an officer of the legislature under their act was compromised. In that report, the commissioner of Alberta requested that the legislature amend their FIPPA to state:

- That I have the power to require public bodies to produce to me records over which solicitor-client privilege and other similar privileges (e.g., litigation privilege, informer privilege) are claimed.
- That I may require those records when, in my opinion, it is necessary to perform my functions (such as when a public body does not provide enough evidence to satisfy me that the records are privileged).
- That solicitor-client privilege or other legal privilege is not waived when the privileged records are provided to me.
- That I may not disclose to the Minister of Justice and Solicitor General, as evidence of an offence, records to which solicitor-client privilege applies.

Under Newfoundland and Labrador’s act, a public body may require the commissioner to examine the original record at a site determined by the head where the head of the public body has a reasonable basis for concern about the security of a record that is subject to solicitor-client privilege. This is consistent with our approach with public bodies when it is necessary to review the records at issue in order to reach our finding on whether the exception for solicitor-client privilege applies. That act, as well as British Columbia’s FIPPA, state that if a public body discloses a record that is subject to solicitor-client privilege to the commissioner at the request of the commissioner, the solicitor-client privilege of the record is not affected by the disclosure.

Amending FIPPA to ensure that the ombudsman has the power to review records over which a claim of solicitor-client privilege has been made to refuse access would preserve an independent review of decisions of public bodies, as is one of the stated purposes of the act, found in clause 2(e) of FIPPA.

## Recommendation 24

Sections 50 and 51 of FIPPA should be amended to clearly express that:

- the ombudsman has the power to require public bodies to produce records over which solicitor-client privilege is claimed
- that the ombudsman may require those records when, in his or her opinion, it is necessary to perform the ombudsman's functions, such as when a public body does not provide enough evidence to establish that the records are privileged
- that solicitor-client privilege is not waived when the privileged records are provided to the ombudsman for purposes of performing his or her duties under the act
- that a public body may require the ombudsman to examine the original record at a site determined by the head where the head of the public body has a reasonable basis for concern about the security of a record that is subject to solicitor-client privilege, and
- that the ombudsman may not disclose to the minister of justice and attorney general, as evidence of an offence, records to which solicitor-client privilege applies

## COMPLAINT FORM

### Issue

The space for a complainant to sign the complaint form and date it is sometimes not completed. Also, when the complainant is authorizing another person to act on their behalf, sometimes the form is mistakenly signed by that person instead of the complainant.

### Discussion

The space for the complainant to add their signature, under the heading "Your Signature," and the date on the complaint form is located at the bottom of the second page of the form. If it were moved to the first page, within the box titled "Your Information," this may increase the likelihood of it being signed and by the correct person.

## Recommendation 25

Incorporate space for the complainant to sign and date the form within the box titled "Your Information" on the first page of the form.

## ADDITIONAL COMPLAINT ABOUT A FAILURE TO PROTECT PERSONAL INFORMATION

### Issue

There should be a right to make a privacy complaint about a failure to protect PI, similar to the right that exists under PHIA for personal health information, which may also be held by a public body.

### Discussion

An individual has a right of complaint about privacy under FIPPA, as follows:

**Complaint about privacy**

**59(3)** An individual who believes that his or her own personal information has been collected, used or disclosed in violation of Part 3 may make a complaint to the Ombudsman.

Under PHIA, in addition to the above complaints, an individual also has a right to make a complaint that a trustee “has failed to protect his or her personal health information in a secure manner as required by this Act.”

Section 41 of FIPPA requires that a public body make reasonable security arrangements to protect PI from risks such as unauthorized access, use, disclosure or destruction. If an individual has reason to believe that a public body has not made reasonable security arrangements to protect their PI, the individual should not have to wait until their PI has been improperly used or disclosed in order to make a complaint.

**Recommendation 26**

A new right of complaint about privacy should be added to enable an individual to make a complaint about a public body that has failed to protect his or her personal information in a secure manner as required by FIPPA.

**INTERJURISDICTIONAL INVESTIGATIONS****Issue**

Personal information may be shared across provincial borders, such as when a citizen living in one province relocates or receives services in another province. There may be situations where, for example, a public body in Manitoba discloses PI to a public body in another province or to the government of Canada. The individual could have a right of complaint under two acts, but the oversight offices conducting the investigations would not have authority under their respective acts to share information related to these investigations.

**Discussion**

PI may be shared across provincial borders and in such circumstances, oversight offices may be engaged in conducting interrelated investigations under their respective information law, but under FIPPA, the ombudsman would not be permitted to share information relating to such investigations.

Some oversight offices are permitted under their laws to share information in such circumstances, including Alberta, Ontario, Yukon and Canada (under the Personal Information Protection and Electronic Documents Act). The information and privacy commissioner of Saskatchewan has proposed an amendment to its FIPPA to enable that office to disclose to another commissioner in Canada with similar powers and duties. As an example, the provisions in Yukon’s health information law are as follows:

**General powers of commissioner**

**92** In addition to the specific duties and powers assigned to the commissioner under this Act, the commissioner is responsible for overseeing how this Act is administered to ensure that its purposes are achieved, and may

(f) exchange personal information and personal health information with any person who, under legislation of another province or Canada, has powers and duties similar to those conferred upon the commissioner under this Act or the Access to Information and Protection of Privacy Act;

(g) enter into information-sharing agreements for the purposes of paragraph (f) and into other agreements with the persons referred to in that paragraph for the purpose of coordinating their activities and exercising any duty, function or power conferred on the commissioner under this Act;

In our comments about PHIA, we have recommended changes to that act to enable the ombudsman to make such disclosures, and we are also doing so for FIPPA.

### **Recommendation 27**

FIPPA should enable the ombudsman to exchange information with another person who under legislation of another province or Canada has powers and duties similar to those conferred upon the ombudsman under FIPPA, for the purpose of coordinating activities and handling complaints involving two or more jurisdictions.

## **DISCLOSURES BY OMBUDSMAN**

### **Issue**

FIPPA does not expressly permit the ombudsman to disclose information in compelling circumstances relating to a risk of serious harm to any individual.

### **Discussion**

FIPPA permits the ombudsman to disclose information obtained in performing duties or exercising powers of investigation under the act, in certain circumstances. This includes when it is necessary to do so to perform a duty or exercise a power, when its necessary to establish grounds for findings and recommendations contained in a report, or to disclose information relating to the commission of an offence.

However, there may be other circumstances in which disclosure would reasonably be considered necessary, such as when it relates to a serious risk of harm to any individual.

### **Recommendation 28**

FIPPA should expressly permit the ombudsman to disclose information obtained in an investigation where the ombudsman reasonably believes that the disclosure is necessary to prevent or lessen a risk of serious harm to any individual.

## OMBUDSMAN’S RIGHT TO BE A PARTY TO ADJUDICATOR’S REVIEW

### Issue

When the ombudsman requests a review by the adjudicator, the ombudsman has a right to be a party to that review, however this right is restricted to matters where “the Ombudsman considers that the review raises an issue of public interest.”

### Discussion

The ombudsman could potentially have an interest in any review he or she requests because the review relates to recommendations made by the ombudsman. The ombudsman’s right to be a party to the review should not be constrained to an issue of public interest. There may be an issue of importance with respect to an individual’s right or a public body’s obligations that does not necessarily raise an issue of broad public interest and the ombudsman should have the right to be a party to such a review.

### Recommendation 29

The ombudsman should have the right to be a party to a review by the adjudicator and the phrase “if the Ombudsman considers that the review raises an issue of public interest” should be deleted.

## OMBUDSMAN’S RIGHT TO INTERVENE AS A PARTY TO AN APPEAL

### Issue

The ombudsman’s right to appeal to court about a refusal of access, as well as to intervene in an appeal by a complainant, was repealed following the previous review of FIPPA. The right to appeal was no longer necessary because instead the ombudsman may request a review by the adjudicator, as is also the case under PHIA. However, the right to intervene in an appeal still remains under PHIA. This inconsistency between FIPPA and PHIA should be addressed.

### Discussion

FIPPA enables a complainant to appeal a public body’s refusal of access to court following an investigation by the ombudsman. Practically, this could occur when the ombudsman has found that a public body’s decision to refuse access was in compliance with FIPPA. A third party may also appeal a public body’s decision to give access to the third party’s information.

When FIPPA was previously amended to add the process for the ombudsman to request a review by the adjudicator, the following provisions were repealed:

#### **Appeal by the Ombudsman**

**68(1)** The Ombudsman may appeal a decision described in subsection 67(1) to the court within the time limit set by subsection 67(3), if the Ombudsman has obtained the consent of the person who has the right of appeal.

**Ombudsman may intervene**

**68(2)** The Ombudsman has a right to intervene as a party to an appeal under section 67.

However, under section 50 of PHIA, the ombudsman still has a right to intervene as a party to an appeal. Based on this, it is unclear why subsection 68(2) was repealed from FIPPA, or whether the intent was to also repeal this right under PHIA. This inconsistency should be addressed.

If the ombudsman were to have the power to intervene in an appeal, it would appear that an amendment to subsection 53(1) would be required to ensure that any statement or report made or opinion given by a person during an investigation by the ombudsman, and any report or recommendation of the ombudsman, would be admissible in evidence in the court proceeding when the ombudsman is a party. Subsection 53(1) currently states:

**Statements and reports not admissible in evidence**

**53(1)** A statement made or an answer given by a person during an investigation by the Ombudsman, and a report or recommendation of the Ombudsman, is inadmissible in evidence in a court or in any other proceeding, except

- (a) in a prosecution for perjury in respect of sworn testimony;
- (b) in a prosecution for an offence under this Act;
- (c) in a review conducted by the adjudicator under this Act when the Ombudsman is a party;
- or
- (d) in an application for judicial review of an adjudicator's order under this Act.

**Recommendation 30**

The inconsistency in the right of the ombudsman to intervene as a party to appeal to court about a refusal of access under PHIA, but not under FIPPA, should be addressed. If the previously repealed subsection 68(2) under FIPPA that provided the ombudsman with this right is added back to FIPPA, an amendment to subsection 53(1) would also be required to ensure that any statement or report made or opinion given by a person during an investigation by the ombudsman, and any report or recommendation of the ombudsman, would be admissible in evidence in a court proceeding when the ombudsman is a party.

**7. ROLE OF INFORMATION AND PRIVACY ADJUDICATOR****ADJUDICATOR'S ORDERS****Issue**

The scope of the orders that the adjudicator may make does not encompass all matters the ombudsman may make recommendations about and ask the adjudicator to review.

**Discussion**

The ombudsman may make any recommendations considered appropriate about a complaint. For example, with respect to privacy, it would appear that an order by the adjudicator would not be able to

address situations in which the ombudsman has made recommendations to a public body to create certain policies to ensure compliance with FIPPA, or to provide privacy training to employees, or to implement reasonable safeguards to protect PI.

On receiving a request from the ombudsman, the adjudicator must conduct a review and further to the review, the adjudicator issues an order, as follows:

**Adjudicator's order**

**66.8(1)** Upon completing a review under section 66.3, the adjudicator must dispose of the issues by making an order under this section.

**Order re giving or refusing access**

**66.8(2)** If the review concerns a decision of the head of a public body to give access or refuse access to all or part of a record, the adjudicator may, by order,

- (a) require the head to give the applicant access to all or part of the record, if the adjudicator determines that the head is not authorized or required to refuse access;
- (b) confirm the decision of the head or require the head to reconsider it, if the adjudicator determines that the head is authorized to refuse access;
- (c) confirm the decision of the head or require the head to refuse access to all or part of the record, if the adjudicator determines that the head is required to refuse access.

**Other orders**

**66.8(3)** If the review concerns any other matter, the adjudicator may, by order,

- (a) require that a duty imposed by this Act be performed;
- (b) confirm or reduce the extension of a time limit under subsection 15(1);
- (c) confirm or reduce a fee, or order a refund of a fee, in the appropriate circumstances;
- (d) confirm a decision not to correct personal information, or specify how personal information is to be corrected;
- (e) require a public body to cease or modify a specified practice of collecting, using or disclosing personal information in contravention of Part 3;
- (f) require the head of a public body to destroy personal information collected in contravention of this Act.

**Limit**

**66.8(4)** If the adjudicator determines that the head is authorized or required to refuse access to a record or part of a record, the adjudicator must not order the head to disclose the record or part of it.

**Order may contain terms or conditions**

**66.8(5)** The adjudicator may specify terms or conditions in an order made under this section.

**Recommendation 31**

The scope of the adjudicator's orders should encompass all matters about which the ombudsman may make recommendations and request a review by the adjudicator.

## 8. OTHER ISSUES

### ADDITIONAL OFFENCES

#### Issue

The offence provision of FIPPA should be expanded to include additional offences that serve as a measure of deterrence and as an appropriate sanction for other types of violations of the act.

#### Discussion

The following are the offences under FIPPA:

#### Offences

**85(1)** Any person who wilfully

- (a) discloses personal information in contravention of Part 3 of this Act;
  - (b) makes a false statement to, or misleads or attempts to mislead, the Ombudsman or another person in performing duties or exercising powers under this Act;
  - (c) obstructs the Ombudsman or another person in performing duties or exercising powers under this Act;
  - (d) destroys a record or erases information in a record that is subject to this Act with the intent to evade a request for access to records; or
  - (e) fails to comply with section 44.1(4) (obligations of an information manager);
- is guilty of an offence and liable on summary conviction to a fine of not more than \$50,000.

Although FIPPA prohibits the use of personal information except for authorized purposes, there is no sanction for intentionally invading someone's privacy by snooping. There should be an offence, similar to the wording used in PHIA, for a person who wilfully "uses, gains access to or attempts to gain access to another person's personal information." This would also be similar to an offence provision in Newfoundland and Labrador's access and privacy law.

Clause 85(1)(d) above makes it an offence where a person wilfully "destroys a record or erases information in a record" with the intent to evade an access request. It should also include concealing a record. Subsection 115(2) of Newfoundland and Labrador's act contains useful wording that could be adopted:

(2) A person who wilfully

- (d) destroys a record or erases information in a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records; or
- (e) alters, falsifies or conceals a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records,

If FIPPA is amended to make it mandatory for a public body to notify individuals and the ombudsman of privacy breaches that may result in real risk of significant harm to the individuals, consideration should be given to creating an offence for a failure to notify.

### Recommendation 32

Expand the types of offences under FIPPA to include where a person wilfully:

- uses, gains access to or attempts to gain access to another person's personal information in contravention of Part 3 of this act
- alters, falsifies or conceals a record that is subject to this act, or directs another person to do so, with the intent to evade a request for access to records

Include an offence for a failure to notify individuals and the ombudsman of a privacy breach that may result in real risk of significant harm to an individual, if it becomes mandatory to provide such notice.

## TIME LIMIT FOR STARTING A PROSECUTION

### Issue

A prosecution of an offence under FIPPA must be started within two years of the commission of the alleged offence. The discovery of an offence may not be made until close to or after that time limit has expired, making a prosecution impossible.

### Discussion

If the time limit for the prosecution of an offence were based on the discovery of an alleged offence, rather than two years from when it was committed, this would provide time for the gathering of evidence for a charge to be laid. An offence may not come to light until several months or years after it was committed. If the alleged offence is not detected soon after commission, the time limit may expire despite that there may be strong evidence for a prosecution.

Under Newfoundland and Labrador's Access to Information and Protection of Privacy Act and Saskatchewan's Health Information Protection Act, there is a two-year time limit based on the discovery of an offence. This would enable sufficient time after such discovery to conduct an investigation and lay a charge.

### Recommendation 33

The time limit for starting a prosecution of an alleged offence under FIPPA should be changed from two years from the commission of the alleged offence, to two years from the discovery of it.

## REVIEW PERIOD

### Issue

FIPPA should be reviewed on a periodic basis to ensure that the act adequately addresses the rights of individuals and the obligations of public bodies, as well as to ensure that the oversight mechanisms are effective.

**Discussion**

Many access and privacy laws across Canada contain a requirement for periodic reviews of the law. This current review of FIPPA was required under the following provision:

**Review of Act in five years**

**98(1)** The minister must undertake a comprehensive review of the operation of this Act, which involves public representations, within five years after an adjudicator is first appointed under section 58.1.

**Recommendation 34**

FIPPA should contain a requirement for the act be reviewed on a periodic basis, such as in five years.

## SUMMARY OF RECOMMENDATIONS TO AMEND FIPPA

### 1. Duty to Document

Number	Recommendation	Page
1	There should be a legislated duty requiring public bodies to document matters related to their deliberations, actions and decisions. This duty could be incorporated into information management laws and subclause 49(a)(ii) of FIPPA should be amended to enable the ombudsman to investigate compliance with requirements respecting the <u>creation</u> , security and destruction of records set out in any other enactment or in a by-law or other legal instrument by which a local public body acts. Alternatively, FIPPA could be amended to create a duty to document.	5

### 2. Proactive Disclosure

Number	Recommendation	Page
2	Consideration should be given to amending FIPPA to increase and strengthen proactive disclosure and open government initiatives. Information that describes records held by public bodies, or records schedules, should be posted online.	8

### 3. Access to Information – Procedural Matters

Number	Recommendation	Page
3	<b>Access to Information – Procedural Matters</b> – On the “Instructions” page of the application form, after an applicant is asked to “Describe the records or information to which you want access to in as much detail as possible,” add a sentence to explain that the form is not to be used for asking questions. Modify the application for access form to provide dedicated spaces for the applicant to fill in their street address/post office box number and their city/town.	8
4	<b>Requests That Involve Personal Health Information to Which PHIA Applies</b> – Subsection 6(1) of FIPPA should be amended to require a public body to treat a FIPPA request that includes PHI to which PHIA applies, as if it were a request under that act, similar to subsection 15.1(1) of Alberta’s FIPPA.	10
5	<b>Abandoned Requests</b> – FIPPA should permit a public body to decide that a request has been abandoned based on specified circumstances, such as when the individual does not provide necessary clarification about their request or accept or pay a fee. The public body should provide notice of this decision in writing to the applicant, explain the reason for the decision, and inform the applicant of the right of complaint about the decision.	11
6	<b>Fees</b> – The Estimate of Costs form should be amended to enable a public body to include the actual cost of providing a copy of records, as set out under clause 5(1)(c) of the Access and Privacy Regulation. This would permit public bodies to calculate for the applicant the total fee including the cost of providing a copy on a storage medium, such as a CD-ROM, DVD or USB flash drive.	13

Number	Recommendation	Page
	With respect to the question of implementing an application fee, we are of the view that this may deter the general public from making requests and that it may not address the issue of time or costs in dealing with multiple and concurrent requests from an individual or an organization.	
7	<b>Fee Waivers</b> – The circumstances for waiving a fee should be expanded to include a broader consideration of fairness to an applicant, by adding a provision such as when waiving a fee would be reasonable and fair in the circumstances.	14
8	<b>Notice to an Applicant and a Third Party Consulted Under Section 33</b> – The complaint process under section 34 should include extra measures to ensure that a third party’s personal or business information does not get released to an applicant without confirming that no complaint has been made within the 21-day time limit. The time frame for an applicant to make a complaint about a decision to refuse access should be changed from 21 days to 60 days.	16

#### 4. Access to Information – Exceptions to Access

Number	Recommendation	Page
9	<b>Privacy of a Third Party</b> – The inconsistency between clause 17(4)(h) of FIPPA and PHIA with respect to the circumstances in which PHI of a deceased individual can be disclosed to a requester should be addressed. Subsection 17(4) should include a provision to disclose to an applicant the business contact information of a third party described in clause 44(1)(x.1). Consider including other types of expenses to be disclosed under clause 17(4)(e).	17
10	<b>Business Interests of a Third Party</b> – Section 18 should be amended to more clearly require a demonstrable harm to a third party’s business interests that could reasonably be expected to result from disclosure of confidential information of a third party. Newfoundland and Labrador, Alberta, Yukon, Nova Scotia and Prince Edward Island have wording that should be used a model to clearly impose a three-part test.	20
11	<b>Labour Relations Interests of a Public Body as an Employer</b> – There should be a specific exception for a public body’s labour relations information as an employer, either within section 28 or as a stand-alone exception.	22
12	<b>Cabinet Confidences</b> – Section 19, Cabinet Confidences, should be changed from a mandatory to a discretionary exception. Subsection 19(2) should include a new provision to enable background information to be disclosed if the decision has been made public, or has been implemented, or five or more years have passed since the decision was made or considered. Subsection 19(2) should include a new provision to permit disclosure by the clerk of the executive council where the clerk is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception. The time frame specified in clause 19(2)(a) after which the exception for cabinet confidences no longer applies should be reduced from 20 years to 15 years or less.	24
13	<b>Advice to a Public Body</b> – Clause 23(1)(b) that applies to consultations and deliberations should be deleted because any such communications that reveal advice would be subject to 23(1)(a), and if advice is not revealed these	28

Number	Recommendation	Page
	<p>communications should not be excepted from disclosure as this is contradictory to the intent of this exception. Subsection 23(2) should provide for the disclosure of:</p> <ul style="list-style-type: none"> <li>• factual material or background information, that is beyond what is currently provided for under subsection 23(2)(f)</li> <li>• information that has been publicly cited as the basis for a public body's decision</li> <li>• information that has been in existence for 15 or more years, reduced from 20 years under clause 23(2)(a)</li> </ul>	
14	<p><b>Information That Will be Made Available to the Public</b> – The time frame in section 32 should be reduced so that a public body may refuse access to information that will be made available to the public within 60 days, instead of 90 days.</p>	29
15	<p><b>Public Interest Override for Exceptions</b> – FIPPA should contain a public interest override to permit disclosure of information subject to discretionary exceptions to be disclosed when it is clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception. The public interest override in the recently amended act in Newfoundland and Labrador could serve as a useful model.</p>	30

## 5. Protection of Privacy

Number	Recommendation	Page
16	<p><b>Protection of Personal Information</b> – The requirements for the protection of personal information need to be updated and strengthened. PHIA should serve as a model for strengthening the requirements in FIPPA.</p>	32
17	<p><b>Mandatory Breach Notification</b> – FIPPA should include requirements to notify individuals and the ombudsman of a privacy breach where a public body reasonably believes that the breach may result in a real risk of significant harm to the individual. Prescribing the types of information to include in notification to individuals may ensure adequate notice is given as a matter of accountability by the public body and fairness to the individual, and it may assist the individual to take any steps necessary to assess and address their own risks.</p>	33
18	<p><b>Secure Destruction of Personal Information</b> – FIPPA should include a requirement to ensure that personal information is destroyed in manner that protects the privacy of the individual the information is about, as is required for personal health information subject to PHIA.</p>	33
19	<p><b>Correction to Personal Information</b> – A public body's response to an individual's request for correction should be required to be in writing. An individual should be permitted to file a concise statement of disagreement about a public body's decision to refuse to correct the record.</p>	34
20	<p><b>No Adverse Employment Action</b> – Subsection 86(2) of FIPPA should not limit the protection for employees to situations in which the disclosure has been made at the request of the ombudsman. Also, no adverse employment action should be taken against employees who exercise their right to make a FIPPA complaint to the ombudsman about their employer. Consideration should be</p>	36

Number	Recommendation	Page
	given to whether the phrase “adverse employment action” should be more clearly set out by including the actions described in Newfoundland and Labrador’s PHIA.	
21	<b>Big Data Analytics</b> – The de-identification processes used by the provincial government to provide information to the repository of de-identified datasets at the Manitoba Centre for Health Policy would support an increased use of big data analytics by the provincial government. If amendments to FIPPA are necessary to enable this, the risks of re-identifying individuals through the linkage of multiple datasets requires that these processes are carefully managed.	37

## 6. Oversight Role of the Ombudsman

Number	Recommendation	Page
22	<b>Rename Title to Information and Privacy Commissioner</b> – FIPPA and PHIA should be amended to change the ombudsman’s title under these acts to information and privacy commissioner and the legislation in Yukon could serve as a model. The acts should also be amended to specifically enable the appointment of a deputy information and privacy commissioner.	38
23	<b>Powers of the Ombudsman Concerning Audits</b> – The provision that enables the ombudsman to require records maintained by a public body to be produced to the ombudsman should be amended to include being able to do so in relation to conducting an audit. The provisions that provide protection for records produced to the ombudsman during an investigation should also include audits.	39
24	<b>Production of Records Over Which Solicitor-Client Privilege is Claimed</b> – Sections 50 and 51 of FIPPA should be amended to clearly express that: <ul style="list-style-type: none"> <li>• the ombudsman has the power to require public bodies to produce records over which solicitor-client privilege is claimed</li> <li>• that the ombudsman may require those records when, in his or her opinion, it is necessary to perform the ombudsman’s functions, such as when a public body does not provide enough evidence to establish that the records are privileged</li> <li>• that solicitor-client privilege is not waived when the privileged records are provided to the ombudsman for purposes of performing his or her duties under the act</li> <li>• that a public body may require the ombudsman to examine the original record at a site determined by the head where the head of the public body has a reasonable basis for concern about the security of a record that is subject to solicitor-client privilege, and</li> <li>• that the ombudsman may not disclose to the minister of justice and attorney general, as evidence of an offence, records to which solicitor-client privilege applies</li> </ul>	42
25	<b>Complaint Form</b> – Incorporate space for the complainant to sign and date the form within the box titled “Your Information” on the first page of the form.	42
26	<b>Additional Complaint About a Failure to Protect Personal Information</b> – A new right of complaint about privacy should be added to enable an individual to	43

Number	Recommendation	Page
	make a complaint about a public body that has failed to protect his or her personal information in a secure manner as required by FIPPA.	
27	<b>Interjurisdictional Investigations</b> – FIPPA should enable the ombudsman to exchange information with another person who under legislation of another province or Canada has powers and duties similar to those conferred upon the ombudsman under FIPPA, for the purpose of coordinating activities and handling complaints involving two or more jurisdictions.	44
28	<b>Disclosures by Ombudsman</b> – FIPPA should expressly permit the ombudsman to disclose information obtained in an investigation where the ombudsman reasonably believes that the disclosure is necessary to prevent or lessen a risk of serious harm to any individual.	44
29	<b>Ombudsman’s Right to be a Party to Adjudicator’s Review</b> – The ombudsman should have the right to be a party to a review by the adjudicator and the phrase “if the Ombudsman considers that the review raises an issue of public interest” should be deleted.	45
30	<b>Ombudsman’s Right to Intervene as a Party to an Appeal</b> – The inconsistency in the right of the ombudsman to intervene as a party to appeal to court about a refusal of access under PHIA, but not under FIPPA, should be addressed. If the previously repealed subsection 68(2) under FIPPA that provided the ombudsman with this right is added back to FIPPA, an amendment to subsection 53(1) would also be required to ensure that any statement or report made or opinion given by a person during an investigation by the ombudsman, and any report or recommendation of the ombudsman, would be admissible in evidence in a court proceeding when the ombudsman is a party.	46

## 7. Role of the Information and Privacy Adjudicator

Number	Recommendation	Page
31	<b>Adjudicator’s Orders</b> – The scope of the adjudicator’s orders should encompass all matters about which the ombudsman may make recommendations and request a review by the adjudicator.	47

## 8. Other Issues

Number	Recommendation	Page
32	<p><b>Additional Offences</b> – Expand the types of offences under FIPPA to include where a person wilfully:</p> <ul style="list-style-type: none"> <li>• uses, gains access to or attempts to gain access to another person's personal information in contravention of Part 3 of this act</li> <li>• alters, falsifies or conceals a record that is subject to this act, or directs another person to do so, with the intent to evade a request for access to records</li> </ul> <p>Include an offence for a failure to notify individuals and the ombudsman of a privacy breach that may result in real risk of significant harm to an individual, if it becomes mandatory to provide such notice.</p>	49

Number	Recommendation	Page
33	<b>Time Limit for Starting a Prosecution</b> – The time limit for starting a prosecution of an alleged offence under FIPPA should be changed from two years from the commission of the alleged offence, to two years from the discovery of it.	49
34	<b>Review Period</b> – FIPPA should contain a requirement for the act be reviewed on a periodic basis, such as in five years.	50