Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

STATUTORY REVIEW OF THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

SUBMISSION TO THE SPECIAL COMMITTEE TO REVIEW THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

November 18, 2015

TABLE OF CONTENTS

PREFACE

For more than two decades, the *Freedom of Information and Protection of Privacy Act* ("FIPPA") has provided a framework for access to information and privacy rights in British Columbia's public sector.

FIPPA's purposes are two-fold: make public bodies more accountable to the public, and protect personal privacy. These purposes are fundamental in our society.

This legislative review is very welcome, as it comes at a critical and opportune time. Access and privacy concerns are at the heart of current events in British Columbia — from large-scale breaches of personal information, to the records management practices of government. New technologies and global trends beyond our borders continue to shape and influence the evolution of B.C.'s privacy and access laws.

This special report makes 20 recommendations for legislative changes to address the current and emerging challenges of our information society and to provide robust protection of privacy and access rights for citizens in the years to come.

November 18, 2015

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

1.0 INTRODUCTION

When the *Freedom of Information and Protection of Privacy Act* ("FIPPA") came into force in 1993, public bodies dealt primarily in paper records. Large scale information-sharing was cumbersome and expensive; e-mail and the Internet were still relatively new business tools.

In 2015, digital technologies and innovations have fundamentally changed how we manage information and records, interact with government, and live our lives. Public bodies at all levels want to increase information sharing, integrate data and facilitate cross-agency sharing of personal information to better serve citizens.

At the same time, citizens expect more services to be available at their fingertips and for public bodies to make information and data more accessible.

Recent events in British Columbia have intensified public focus on access to information and privacy, spotlighting the need for updating the legislation. A legislated duty to document, mandatory breach notification and reporting, oversight of the destruction of records, enhanced penalties, and stronger proactive disclosure requirements are among the major recommendations for change set out in this report.

FIPPA was designed for a paper-based operating environment. The transition to the digital age has created new challenges and opportunities for privacy and access rights of citizens. I sincerely believe FIPPA has to change to deal with this major shift.

This submission organizes our recommendations under three key themes: *transparency*, *accountability*, and *effective oversight.* Each recommendation includes a discussion of the issue at hand. Where appropriate, we have also included relevant information about trends in other jurisdictions and noted whether the recommendation has been made to a previous Special Review Committee.

2.0 RECOMMENDATIONS TO AMEND FIPPA

2.1 PROMOTING TRANSPARENCY AND OPENNESS

Access rights offer a way for citizens to inform themselves about the business of their government which impacts them.

Citizens want to know such information as: why did the government pursue one course of action or another? What is the business case for this decision? What considerations informed how my tax dollars are being spent? Citizens can and should be able to ask and receive answers to these and other questions.

Access to information legislation provides important requirements that ensure the accountability of public bodies. The recommendations in this section are aimed at improving those requirements so that transparency and accountability of government agencies are further enhanced.

➢ CREATE A DUTY TO DOCUMENT

Issue
FIPPA does not currently require public bodies to *create* records regarding government information to document key decisions and actions.

Discussion
Good governance and good record keeping go hand in hand.

Effective record keeping requires that appropriate records be retained. I have addressed that issue in several reports issued by my Office.[1]

Good records management also requires, in certain circumstances, that records be created. I have used the phrase "duty to document" to describe this obligation.

[1] OIPC BC, Investigation Report F15-03, "Access Denied: Record Retention and Disposal Practices of the Government of British Columbia", October 22, 2015, at: https://www.oipc.bc.ca/investigation-reports/1874.
OIPC BC, Investigation Report F13-01, "Increase in No Responsive Records to General Access to Information Requests: Government of British Columbia", March 04, 2013, at: https://www.oipc.bc.ca/investigation-reports/1510.
OIPC BC, Special Report, "A Step Backwards: Report Card On Government's Access To Information Responses
April 1, 2013 – March 31, 2014", May 16, 2011, at: https://www.oipc.bc.ca/special-reports/1696.

The starting point for considering the duty to document is a discussion of the concept of records, which the recently passed *Information Management Act* (IMA) appropriately calls government information.[2]

The definition in the IMA of what constitutes government information is thorough, and includes two main (of five) elements:

> (b) Information that documents a decision by a government body respecting a course of action that directly affects a person or the operations of the government,
>
> (c) Information that documents or supports the government body's organization, policies, procedures, transactions or operations.[3]

These elements are vital to enabling government to track and retain evidence of transactions and decisions that may be subject to, among other matters, financial audits or legal challenges. They are the same elements that should underlie a duty to document for *all* public bodies.

While this definition in the IMA sets out the mechanisms for the retention of these critical records, it leaves unaddressed the need to create them in the first instance. A comprehensive legislated duty to document for *all* public bodies should build on and extend the definition of government information in the IMA.

In a paper-based environment, one-on-one phone calls, meetings, memos and reports were the dominant form of communication. In the vast majority of cases, important information was written in a memo or report, assigned a file number, and filed by a staff person in each work unit assigned to that purpose. Access requests were dealt with by reviewing paper files, photocopying the information, and releasing it, subject to the exceptions in FIPPA. This process ensured that records were created in a manner that gave them meaning and structure, and records were easily retrievable when needed to review a decision or in response to an access request.

The digital age changed the method of communication. Phone calls and meetings still occur, but email communication has become the dominate form of transactions and communications. The result has been an increase in the volume of records that are created and challenges in the filing of electronic records. Yet email records often lack the structure and content that is necessary for them to provide "reliable and dependable" evidence of a public's body's actions and decisions.[4] A duty to document addresses this issue by focusing attention on the need to create full and accurate records.

---

[2] The IMA is not yet in force in BC.
[3] Section 1 of the IMA.
[4] Queensland State Archives, "Create and Capture Module", at: http://www.archives.qld.gov.au/Recordkeeping/Digital/Pages/CreateCapture.aspx.

My submission to you today is based on the premise that there should be a clear and positive duty to **create** records of government information consistent with the definition in the new IMA. Without this, our collective ability to examine the operations of government cannot have full force and effect.

This issue has been highlighted by my Office in numerous reports. In 2013, I published an investigation into complaints about "no responsive records" replies to access requests made to the B.C. government.[5] In that report, we recommended that government create a duty within FIPPA to document key decisions of government to demonstrate its commitment to public accountability. In other reports, I have recommended that government adopt a duty to document in order to preserve the historical legacy of government decisions and as a key records management component of proactive disclosure programs.[6]

A number of statutes in B.C. contain provisions respecting the creation of records or information (a duty to document), including the *Budget Transparency and Accountability Act*, the *Public Service Act*, and the *Environmental Management Act*, to name a few. While these provisions serve specific purposes, they are limited.

The public interest would be advanced by adding a general provision to FIPPA that clearly defines and addresses the responsibility of all public bodies to create documents in B.C.. This definition should build on the existing definition of "government information" in the IMA and it would extend to all public bodies, from the Ministry of Health to BC Ferries.

A general duty to document exists in other jurisdictions. In the Canadian context the Committee reviewing Newfoundland and Labrador's Access to *Information and Protection of Privacy Act* recommended the adoption of a duty to document and the government has committed to do so.[7]

Australian jurisdictions and New Zealand have broad legal requirements to create full and accurate records. New Zealand's *Public Records Act* obligates public offices to "create and maintain full and accurate records of its affairs,

---

[5] OIPC BC, Investigation Report F13-01, "Increase in No Responsive Records to General Access to Information Requests: Government of British Columbia", March 04, 2013, at: https://www.oipc.bc.ca/investigation-reports/1510.

[6] OIPC BC, Investigation Report F15-03, "Access Denied: Record Retention and Disposal Practices of the Government of British Columbia", October 22, 2015, at: https://www.oipc.bc.ca/investigation-reports/1874; OIPC BC, Investigation Report F11-02, "Investigation Into The Simultaneous Disclosure Practice Of BC Ferries", May 16, 2011, at: https://www.oipc.bc.ca/investigation-reports/1243.
OIPC BC, Special Report, "A Failure To Archive - Recommendations To Modernize Government Records Management", July 22, 2014, at: https://www.oipc.bc.ca/special-reports/1664.

[7] "Davis Government to Implement ATIPPA Recommendations". at https://www.pcpartynl.ca/issue/access-to-information/ .

considering normal, prudent business practices."[8] The New South Wales *State Records Act* requires each public office to "make and keep full and accurate records of the activities of the office."[9]

These jurisdictions have further delineated the duty to document in standards and policies that allow public bodies to identify records necessary for their business needs, accountability requirements and community expectations. For example, the core records in the Ministry of Health will be very different from the core records of the Ministry of Energy and Mines. Under standards and policies, the heads of public bodies determine what records need to be created in order to document their business activities and then determine how those records will be retained.

There are a number of design elements in these systems, but they allow for employees to know when and how to document business activities and retain records to ensure accountable decision-making. In short, the legislative framework in these jurisdictions set out a road map that is practical, rational and meets the bar of good governance.

An alternative approach is the Treasury Board of Canada Secretariat's policy directive requiring deputy heads to ensure:

> that decisions and decision-making processes are documented to account for and support the continuity of departmental operations, permit the reconstruction of the evolution of policies and programs, and allow for independent evaluation, audit and review.[10]

A final point to note about a duty to document is that the creation of records does not necessarily mean that the records will be *disclosed* in response to an access request. Access to information law provides that, in some instances, the disclosure of information would not be in the public interest. FIPPA provides a carefully crafted set of exceptions from disclosure where the release of information would, for example, be harmful to law enforcement, intergovernmental relations, or the business interests of a third party. The exceptions in FIPPA will continue to apply where a legislated duty to document exists.

---

[8] Section 17 of the New Zealand *Public Records Act 2005*, at: http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345729.html.

[9] Section 12 of the New South Wales State Records Act 1998, at: http://www.austlii.edu.au/au/legis/nsw/consol_act/sra1998156/.

[10] Treasury Board of Canada Secretariat. *Policy on Information Management*. Retrieved from the Treasury Board of Canada Secretariat website: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742&section=HTML.

Previous recommendations
In the 2010 submission from the Office of the Information and Privacy Commissioner (OIPC) to the Special Committee, my Office noted that we had investigated hundreds of complaints concerning the fact that a requested record did not exist, because it was never created. In response to these concerns, we recommended a duty to document be added to FIPPA. The Special Committee did not address the matter.

However, since then, the government has twice suggested the Special Committee consider a legislated duty to document. The first was in response to my 2013 investigation report, *Increase in No Responsive Records to General Access to Information Requests: Government of British Columbia*.[11] The second was government directly asking the Special Committee to consider this issue in response to the concerns raised in my recently released investigation report, *Access Denied: Record Retention and Disposal Practices of the Government of British Columbia*.[12]

Given its importance for good governance and accountability, we urge the Committee recommend that a general duty to document be added to FIPPA.

While I have previously stated that a duty to document could be placed in information management legislation, there are compelling reasons why FIPPA should contain this requirement. The IMA only applies to ministries and designated government agencies whereas FIPPA applies to all public bodies. Further, there is an integral connection between the duty to document and access rights. Last, FIPPA contains the oversight framework that is needed to ensure that the duty to create and retain records has the appropriate oversight.

Conclusion
In the digital era, records management is challenging to a vast number of public officials. However, public confidence in the operation of government and public bodies requires that records be created consistent with the definition of government information in the IMA.

FIPPA should be amended to include a duty to document. This would be preferable to amending the IMA because FIPPA covers all public bodies and an independent oversight mechanism is already in place.

---

[11] OIPC BC, Investigation Report F13-01, "Increase in No Responsive Records to General Access to Information Requests: Government of British Columbia", March 04, 2013, at: https://www.oipc.bc.ca/investigation-reports/1510.
[12] OIPC BC, Investigation Report F15-03, "Access Denied: Record Retention and Disposal Practices of the Government of British Columbia", October 22, 2015, at: https://www.oipc.bc.ca/investigation-reports/1874.

Recommendation 1:

Add to Part 2 of FIPPA a duty for public bodies to document key actions and decisions based on the definition of "government information" in the *Information Management Act*.

➢ Restoring Access Rights Removed by the Courts

Issue
A key element of transparency and accountability is the public's right to access information related to decisions made by public bodies. This right has been eroded by the broad interpretation of the exception to access provided for in s. 13 of FIPPA relating to "policy advice or recommendations" made to a public body.

Discussion
Section 13 of FIPPA provides an exception to access to information for information which would reveal advice or recommendations developed by or for a public body or Minister. My office has historically interpreted the phrase "advice or recommendations" as being intended to convey one idea; they are similar terms that are often used interchangeably to convey suggested actions for acceptance or rejection during a deliberative process.

However, recent court decisions[13] have interpreted this section such that the words "advice" and "recommendations" must be taken to have different meanings; having the practical effect of significantly broadening the application of this exception to access. As a consequence, s. 13 is now being interpreted to not only exempt the advice or recommendations describing potential alternative courses of actions, but also apply to the facts and information compiled in the course of making those recommendations.

This interpretation broadens the application of s. 13 such that any document compiled in the course of considering alternative options is effectively exempt from disclosure under FIPPA.

This frustrates the intended balance that the Legislature sought in enacting the provision: to protect the full and frank provision of advice to a decision maker by protecting the policy advice or recommendations from being released, while enabling the release of the factual material underpinning the advice.

---

[13] *John Doe v. Ontario (Finance)*, 2014 SCC 36; *Insurance Corporation of British Columbia v. Automotive Retailers Association*, 2013 BCSC 2025; *Provincial Health Service Authority vs. British Columbia (Information and Privacy Commissioner)*, 2013, BCSC 2322.

A public body ought to have confidence that advice provided to it is free from any chill that may result from concern about access to information. At the same time, factual material collected by a public body in the course of public business should not be considered confidential or secret.

Similarly, this exception should not apply to professional or technical opinions upon which advice or recommendations are based. Such expert opinions are similar to factual material in that they provide the underpinning for policy advice, but they do not, in themselves, constitute advice. Rather, they are opinions expressed by experts in response to technical questions.

The historical interpretation of my Office that this exception does not apply to factual information is buttressed by the Legislature's clear intention that such material was not to be withheld under s. 13:

> 13(1) The head of a public body may refuse to disclose to an applicant information that would reveal advice or recommendations developed by or for a public body or a minister.
>
> (2) The head of a public body must not refuse to disclose under subsection (1)
>
> (a) any factual material,
>
> (...)
>
> (Emphasis added)

In enacting s. 13, the Legislature sought to protect from access by the public the advice and recommendations that suggested a particular course of action. It did so by using the common and plain meaning of the phrase "advice or recommendations" to convey a single idea. However, this plain language drafting, which should generally be encouraged of government, has left the door open to an overly broad interpretation by the courts. This has had the effect of frustrating the clear intention of the Legislature that factual material must not be subject to this exception and has diminished the public's right to information.

Previous recommendations

Discussions about s. 13 date back to the 2004 Special Committee to Review FIPPA. That Committee found that there was a compelling and urgent need to restore the public's legal right to access to any factual information.[14]

---

[14] Special Committee to Review the *Freedom of Information and Protection of Privacy Act*, *Enhancing the Province's Public Sector Access and Privacy Law*, Report 2004, Legislative Assembly of British Columbia, at: https://www.leg.bc.ca/content/legacy/web/cmt/37thParl/session-5/foi/reports/PDF/Rpt-FOI-37-5-EnchanceProvPubSectAccessPrivacyLaw-2004-MAY-19.pdf , at p. 20.

However, government did not act on that Committee's recommendation and my Office made the same submissions with respect to s. 13 in our submission to the Special Review Committee in 2010. That Committee considered the array of recommendations to revise FIPPA to narrow the interpretation of the section, but ultimately decided not to recommend an amendment.[15]

Conclusion

In the five years since the Report of the 2010 Special Committee, decisions of the Supreme Court of BC as well as a recent decision of the Supreme Court of Canada have continued to broaden the interpretation of s. 13. The effect has been to curtail the public's right to access factual information which served as the basis for policy decisions of public bodies.

FIPPA should be amended to fulfill the original legislative intent of s. 13 by ensuring that advice or recommendations suggesting a particular course of action should be exempt from access to information requests. This would enable public servants or elected officials to freely discuss policy alternatives and make decisions based on those alternatives, while withholding the public's right to the factual material that led to those recommendations.

Recommendation 2:

Section 13(1) of FIPPA should be amended to clarify the following:

- **"advice" and "recommendations" are similar and often interchangeably used terms, rather than sweeping and separate concepts;**
- **"advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process;**
- **the "advice" or "recommendations" does not apply to the facts upon which the advice or recommendation is based; and**
- **the "advice" or "recommendations" does not apply to factual, investigative, or background material, for the assessment or analysis of such material, or for professional or technical opinions.**

[15] Special Committee to Review the *Freedom of Information and Protection of Privacy Act*, Report May 2010, Legislative Assembly of British Columbia. https://www.leg.bc.ca/content/legacy/web/cmt/37thParl/session-5/foi/reports/PDF/Rpt-FOI-37-5-EnchanceProvPubSectAccessPrivacyLaw-2004-MAY-19.pdf, at p. 16.

➢ BRING ENTITIES CREATED BY PUBLIC BODIES UNDER FIPPA

Issue
A purpose of FIPPA is to make public bodies more accountable to the public. However, some corporations or other agencies created by public bodies are not covered under FIPPA. This creates an accountability gap for these entities.

Discussion
There is no sound policy reason as to why corporations or other agencies created by public bodies should not fall under FIPPA. This issue first emanated from post-secondary educational institutions creating subsidiary corporations.

Some institutions believe, for example, that the financial or competitive interests of these corporations may be jeopardized by being subject to access to information. However, FIPPA already addresses this concern because it authorizes public bodies to refuse to disclose information that is harmful to the financial or economic interests of a public body, and it requires public bodies to refuse to disclose information that would be harmful to third party business interests.[16]

FIPPA contains a different set of rules on this issue for local government bodies. Corporations or other organizations created by local government bodies *are* covered:

> any board, committee, commission, panel, agency or corporation that is created or owned by a body referred to in paragraphs (a) to (m) and all the members or officers of which are appointed or chosen by or under the authority of that body.[17]

These entities are held accountable under FIPPA when they are formed by "local government bodies", but not when they are formed by other "public bodies". This creates a lack of accountability for the public when it comes to an entity that is formed by a public body such as a wholly owned subsidiary corporation of post-secondary institutions.

In June 2014 and October 2011, I wrote to the relevant Ministers to ask that an amendment be drafted to FIPPA to ensure that these entities for all public bodies are covered by FIPPA.[18] The government has not proposed any amendments to resolve this accountability gap, nor has it explained why it has not.

---

[16] Sections 17 and 21.
[17] Schedule 1, paragraph (n) definition of "local government body".
[18] For example, see letter from Commissioner Denham to Honourable Dr. Margaret MacDiarmid, October 20, 2011, at: https://www.oipc.bc.ca/public-comments/1138.

Similarly, in December 2013, I considered whether the BC Association of Chiefs of Police (BCACP) and the BC Association of Municipal Chiefs of Police should be added to FIPPA as public bodies. Those associations work closely with the Ministry of Justice and engage in public policy discussions regarding law enforcement. They exert considerable influence over law enforcement decisions by government and police forces in B.C.. However, they are not subject to the same access to information obligations as other publically–funded entities.

In April 2014, I wrote to government recommending that these associations be added as public bodies to Schedule 2 of FIPPA. However, even though the Associations themselves agreed that this would be appropriate, government has not acted on this recommendation.

Previous recommendations
My office made this recommendation to the Committee in 2010.[19] The Special Committee recommended that the definition of "public body" be expanded to include any corporation that is created or owned by a public body.[20]

Conclusion
Corporations or other organizations set up by public bodies are conducting public business. As such they should be subjected to FIPPA and held accountable for their use of public resources.

This will improve accountability and transparency for the public and create consistency with the requirements for local government bodies.

Recommendation 3:

Amend FIPPA to move paragraph (n) of the definition of "local government body" into the definition of "public body" in Schedule 1, so that entities such as subsidiaries of educational bodies and the BCACP fall within the scope of FIPPA.

[19] Recommendation 11(a), Submission of the A/Information and Privacy Commissioner to the Special Committee to Review the Freedom of Information and Protection of Privacy Act, March 15, 2010.
[20] Recommendation 4, Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act, 2nd Sess., 39th Parl., May, 2010.

➢ PUBLISH THE CATEGORIES ESTABLISHED FOR PROACTIVE DISCLOSURES

Issue
Public bodies are required by s. 71 of FIPPA to establish categories of information for proactive disclosure without requiring an access request. However, they are almost universally failing to meet this requirement. In addition, the Minister responsible for FIPPA, who has the prerogative under s. 71.1 to establish such categories for proactive disclosure, has not implemented this provision in a way that the public can easily access and understand.

Discussion
Proactive disclosures involve a public body publishing information or otherwise making it generally available to the public. This improves the transparency of the public body's operations and governance and it promotes an informed citizenry. Proactive disclosures also create efficiencies and cost savings in the administration of access requests for public bodies.

Two changes were made to FIPPA in 2011 with respect to proactive disclosure. The first was an amendment to s. 71. Prior to the amendment, s. 71 granted discretionary authority to the head of a public body to prescribe categories of records to be made available to the public, on demand, without a request for access. In 2011, s. 71 was amended to make it mandatory to establish such categories.

The second change was the addition of a discretionary authority, for the Minister responsible for FIPPA, to establish categories of records that Ministries must make available to the public without an access request. This amendment provides a clear opportunity for leadership of proactive disclosure by government.

In 2013, I published a report evaluating Government of British Columbia's open government initiative.[1] In that report, I made a number of recommendations to government on this subject. However, government has not acted on these recommendations and public bodies continue to fail in their duty to proactively release information.

To the best knowledge of my Office, no categories have been established under ss. 71 or 71.1. Some information has been published on the government's Open Information website (for example, summaries of flight and travel expenses for the Premier, Ministers, and Deputy Ministers). However, there is no way for the public to determine whether an established category exists or whether these are merely ad hoc disclosures. Some data sets have also been released, but again it is not clear whether they were released as a category established under ss. 71 or 71.1.

In contrast, by policy, the federal government requires proactive disclosure for some important categories of records. For example, the contracting policy requires deputy heads of public bodies to "publicly disclose quarterly, within one month after the close of each quarter, contracts entered into or amendments valued at over $10,000."[1] This policy is supported by the Treasury Board's *Guidelines on the Proactive Disclosure of Contracts*, which include details such as data elements to be disclosed, amendments that must be disclosed, and the publication of contracts on departmental websites. The policy also holds the department's chief financial officer responsible for monitoring this proactive disclosure.[1]

Québec also sets out a list of personal information that is designated as public information. It includes information such as the salary for a member of a board of directors, or of the management of a public body, or a deputy Minister, information about a service provider who has entered into a contract with a public body, and the terms and conditions of such a contract.[1]

Previous recommendations
Discussions about proactive disclosures date back to the Special Committee to Review FIPPA, which issued its report in 1999. That report included a recommendation to amend s. 2 of FIPPA to support "open and ready access to government information".[1]

In 2004 and again in 2010, my Office recommended amendments to FIPPA that would require public bodies to proactively disclose records. The respective Committees agreed. In 2004 the Special Committee made this recommendation:

> Add a new s. at the beginning of Part 2 of the Act requiring public bodies — at least at the provincial government level — to adopt schemes approved by the Commissioner for the routine disclosure of electronic records, and to have them operational within a reasonable period of time.[1]

In 2010, the Special Committee made this recommendation:

> Add a new section at the beginning of Part 2 of the Act requiring public bodies to adopt schemes approved by the Commissioner for the routine disclosure of electronic records, and to have them operational within a reasonable period of time.[1]

The changes made in 2011 have not proven adequate.

Conclusion
The public needs greater transparency from government to understand how ss. 71 and 71.1 are being implemented in regards to proactive disclosure. FIPPA should include a requirement that the head of a public body or the Minister

publish any established categories of records for public access. Each public body or Ministry should be required to publish its list of established categories in one easily accessible place.

I continue to recommend that public bodies should be making proactive disclosures on:

- Travel and hospitality expenses of executive staff and ministers. The disclosed information should include the date of the event, destination, and expenses relating to flight, other transportation, accommodations, meals and incidentals, and the total amount spent for that particular purpose or event.

- Information about contracts over $10,000. Contract information should include the parties to the contract, the purpose, value and duration of that contract, and information about the process followed to award the contract. This information should be published on a quarterly basis.

- Final reports or audits on the performance or efficiency of a public body's policies, programs or activities.

- Calendar information of ministers and senior officials. This release should contain the names of participants, the subject and date of external meetings and be published, at minimum, on a monthly basis.

This information should be published in a manner that is open and accessible, easy to find, easy to search, easy to use, and easy to reuse.

Recommendation 4:

Amend ss. 71 and 71.1 of FIPPA to require the publication of any categories of records that are established by the head of a public body or the Minister and made available to the public without an access request. This list should include links to relevant information or records.

➢ Assure Anonymity for Applicants Making Access Requests

Issue

Government currently has a policy that provides anonymity for applicants who make access to information requests to protect them from possible discriminatory treatment. However, this policy does not extend to applicants requesting information from public bodies outside of core government (*e.g.,* schools, health

authorities, universities), leaving the potential for applicants to be at risk of being identified. Moreover, since this government policy has not been legislated it could change with successive governments, leaving all applicants vulnerable.

Discussion
Applicants who make access to information requests expect anonymity. However, FIPPA does not require public bodies to assure that applicants' identities will be protected by public bodies. This both opens the applicant to possible discrimination and it appears to negatively influence response times, as we saw in the 2009 OIPC report on the *Timeliness of Government's Access to Information Responses*. That investigation indicated that there were slower response times to requests made by political parties, media, and advocacy groups, showing that these applicants' identities may have affected the timelines of the responses to their requests.

Newfoundland and Labrador included a provision for anonymity in access requests in the recent report of its legislative review of its *Access to Information and Protection of Privacy Act* (AIPPA). Section 12 ensures anonymity for applicants, for "the name or type of applicant", until the final response is sent.[21] It limits who can know the identity of a requester to "the individual who receives the request on behalf of the public body, the coordinator, the coordinator's assistant and, where necessary, the commissioner". It also contains an exception to anonymity when the applicant is requesting personal information or where the applicant's name is necessary for responding to the request. Nevertheless, in these circumstances, it requires that disclosure of the applicant's name be "limited to the extent necessary to respond to the request".[22]

Section 4(2.1) of the federal *Access to Information Act* also requires that responses to access requests happen "without regard to the identity of a person making a request for access".

Previous recommendations
In 2004, the Special Committee reviewing FIPPA recommended a legislative amendment protecting anonymity for access requestors. My office recommended a right to anonymity to the Special Committee reviewing FIPPA in 2010 and the 2010 Special Committee made the same recommendation. However, government recommended against it in the review, stating that the issue had already been addressed through policy.

Conclusion
Anonymity for applicants should be protected in FIPPA. Government policies are not sufficient to cover all public bodies and an amendment to FIPPA would make it clear for public bodies and applicants alike that anonymity supports the

[21] Section 12, *Access to Information and Protection of Privacy Act*, SNL 2015.
[22] Sections 12(2) and 12(3).

underlying purposes of FIPPA. The amendment should provide an exception in situations where an applicant is applying for their own personal information.

Recommendation 5:

Amend FIPPA to require public bodies to ensure that the name and type of applicant is only disclosed to the individual at the public body that receives an access request on behalf of that public body, while providing for limited exceptions where the applicant is requesting their own personal information or where the name of the applicant is necessary to respond to the request.

➢ AUTHORIZE THE PUBLICATION OF NON-STATUTORY INVESTIGATION REPORTS

Issue

Government has stated that investigation reports conducted by non-statutory authorities cannot be posted online because they contain personal information that cannot be disclosed outside of Canada. However, the public interest in online publication can outweigh the privacy interests of individuals whose personal information is disclosed in a report.

Discussion

From time to time, government appoints a non-statutory investigator to conduct an investigation and produce a report on a matter that is of interest to the public. These types of investigation reports may contain personal information. At the same time, there is often considerable public interest in these reports.

For example, when the government received the McNeil Report regarding the review of the Ministry of Health firings, it did not make that report available online. Instead the government posted a news summary on December 19th, 2014 of some of the findings in the report, and — citing FIPPA — stated that the report could not be made available online.[23] For similar reasons, the Mingay Report, which was released in June 2014 and examined a failure to meet disclosure requirements for the payment of Kwantlen Polytechnic University executives, was also not posted online.

FIPPA has a two-fold purpose: to make public bodies accountable to the public and to protect personal privacy.[24] At times, these two objectives need to be

[23] Government of British Columbia, "Government accepts findings of independent HR review", news release, 19 December, 2014, at: https://news.gov.bc.ca/stories/government-accepts-findings-of-independent-hr-review.

[24] See s. 2 of FIPPA.

considered together. FIPPA was never intended to shield the government from accountability; rather, one of its key purposes is to promote accountability.

The Minster responsible for FIPPA has the authority to order that a report can be disclosed outside of Canada under s. 33.1(3). This discretionary authority has been exercised on a number of occasions,[25] but was not used for the reports mentioned above, despite the public's interest in these reports.

The present legislation is inadequate because it does not explicitly provide the opportunity to consider the public interest in disclosing such reports. It does not allow the head of a public body to weigh those interests against the privacy interests of any person whose personal information is disclosed in the report.

Conclusion
Given that the purpose of non-statutory investigation reports is to provide information to the public about a specific situation, the head of a public body should be able to make them available online when, in that person's informed and objective opinion, the public interest in the disclosure and access to the report outweighs the privacy interests of any person mentioned in the report.

Recommendation 6:

Add an exception to s. 33.1(1) that states that a public body may disclose personal information inside or outside of Canada, if the information is contained in a non-statutory investigation or fact-finding report commissioned by a public body, where the head of the public body concludes the public interest in disclosure outweighs the privacy interests of any person whose personal information is contained in the report.

[25] At least four reports have been published online under and Order pursuant to s. 33.1(3) from various public bodies, including for the Minister of the Environment (Order M276), the Minister of Citizen's Services (Order M030), the Minister of Education (Order M351), and the Minister of Finance and Ministry of Advanced Education (Order M450). See the Ministry of Technology, Innovation, and Citizens' Services, "Ministerial Orders under Section 33.1(3)", at http://www.cio.gov.bc.ca/cio/priv_leg/foippa/order_summaries/min_orders.page.

2.2 PROMOTING ACCOUNTABILITY

Accountability is a topic that is receiving considerable attention from privacy professionals across Canada and around the world, as they seek ways to ensure the sound management of our citizens' personal information.

What does accountability mean? In the context of privacy, accountability means that a public body accepts and is able to demonstrate that it is fulfilling its responsibilities to safeguard the personal information under its control. The responsible management of personal information is at the heart of accountability. Privacy management programs, including mandatory breach notification, are expected by citizens and contained in data protection statutes in leading jurisdictions.

➢ REQUIRE PRIVACY MANAGEMENT PROGRAMS

Issue
Currently there is no requirement under FIPPA for public bodies to implement the essential elements of a privacy management program. Citizens often have little to no choice about providing their personal information to public bodies, regardless of whether that entity has a poor or good record of protecting the privacy of citizens.

Discussion
A privacy management program is, for a person's private information, very similar to a financial management program, dealing with public finances.

This is an issue that my Office addressed in the most recent review of the *Personal Information Protection Act* (PIPA). The Special Committee agreed in that review that privacy management programs should be mandated under PIPA.[26]

The case for the inclusion of a privacy management program in FIPPA is arguably even stronger than it is under PIPA. In the private sector, citizens can be selective about who they trust with their personal information, they can seek one of many private sector providers. In contrast, in most instances, there is no choice in the public sector.

FIPPA is founded upon the Organization for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and*

---

[26] Recommendation 1, *Special Committee to Review the Personal Information Protection Act*, , February 2015, Report, 3rd Session, 40th Parliament at: https://www.leg.bc.ca/content/legacy/web/cmt/40thparl/session-3/pipa/reports/PDF/Rpt-PIPA-40-3-Report-2015-FEB-06.pdf.

Transborder Flows of Personal Data.[27] One of the key OECD principles is accountability, which is about public bodies taking measures to give effect to all of the privacy principles.

The OECD has recently revised its *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* to describe privacy management programs as "the core operational mechanism through which organizations implement privacy protection".[28] The OECD framework also states that public bodies should be able to demonstrate their privacy management programs to the Information and Privacy Commissioner "as appropriate".[29]

In 2013, my Office published guidance on privacy management programs for the public sector.[30] When public bodies properly implement privacy management programs, employees have the training and tools to take a more comprehensive approach to protecting personal information in accordance with the requirements of the Act.

Our office regularly confronts the problems and harms associated with an ad hoc approach to privacy management through complaints, investigations and audits. For example, my investigation into the use of employee monitoring software in the District of Saanich concluded that if the District had made a Privacy Officer responsible for meeting its responsibilities under FIPPA, and trained staff in those responsibilities, it may have prevented the introduction of the privacy-intrusive software.[31]

In addition, my recent examination of breach management practices within seven health authorities further highlights the need for compliance monitoring and risk assessment, greater awareness of staff responsibilities through training, and stronger governance and leadership.[32] Presently **none** of these requirements — training, naming an individual responsible for privacy, policy development, creating a point of contact for the public, and active monitoring — are required under FIPPA.

---

[27] OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, published in 1980 and Revised in 2013, at: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. The OECD privacy principles are: collection limitation; data quality; propose specification; use limitation; security safeguards; openness; individual participation, and accountability.

[28] OECD, at p. 5.

[29] See paras. 15(b) and 15(c) of the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.*

[30] OIPC, "Accountable Privacy Management in BC's Public Sector", June 26, 2013, at https://www.oipc.bc.ca/guidance-documents/1545. The OIPC has also published similar guidance for the private sector.

[31] See Recommendation 5, OIPC BC, Investigation Report F15-01, "*Use of Employee Monitoring Software by the District of Saanich*" March 30, 2015, at: https://www.oipc.bc.ca/investigation-reports/1775.

[32] OIPC BC, *Examination of British Columbia Health Authority Privacy Breach Management*, September 30, 2015, at: https://www.oipc.bc.ca/special-reports/1864.

Previous recommendations
This recommendation has not been made to a previous Special Committee. However, PIPA contains some accountability provisions,[33] and FIPPA should *at least* contain these same provisions while also permitting public bodies to tailor their privacy management programs to their operations. In 2015, the Special Committee to Review PIPA recommended additional accountability measures to modernize PIPA and keep pace with international developments in this area.[34]

Conclusion
Public bodies should be required to have the essential elements of a privacy management program in place. As discussed, these elements should meet or exceed the recommended requirements in PIPA. FIPPA should set out the core elements of privacy management programs that public bodies should be obligated to implement. This will set clear expectations for public bodies, establish defined criteria for oversight and, most importantly, safeguard the personal information of British Columbians by proactively requiring a minimal set of privacy controls.

Recommendation 7:

Add to FIPPA a requirement that public bodies have a privacy management program that:

- **designates one or more individuals to be responsible for ensuring that the public body complies with FIPPA;**
- **is tailored to the structure, scale, volume, and sensitivity of the personal information collected by the public body;**
- **includes policies and practices that are developed and followed so that the public body can meet its obligations under FIPPA, and makes policies publicly available;**
- **includes privacy training for employees of the public body;**
- **has a process to respond to complaints that may arise respecting the application of FIPPA; and**
- **is regularly monitored and updated.**

[33] Part 2 of PIPA contains general rules respecting protection of personal information by organizations, including a general responsibility for personal information under their control, a requirement to designate someone responsible for ensuring compliance with PIPA, developing policies and practices necessary to meet the obligations of the organization under PIPA, and developing a process for responding to complaints regarding the application of PIPA.
[34] Recommendation 1, "*Special Committee to Review the Personal Information Protection Act*", February 2015, Report, 3rd Session, 40th Parliament, at: http://www.leg.bc.ca/cmt/40thparl/session-3/pipa/reports/PDF/Rpt-PIPA-40-3-Report-2015-FEB-06.pdf.

➢ ADD A REQUIREMENT FOR BREACH NOTIFICATION AND REPORTING

Issue
Privacy breaches compromise the personal information of individuals. Breaches can lead to significant harm for individuals and can damage trust in public bodies. However, FIPPA does not currently require breach notification and reporting; instead, public bodies notify affected individuals and report to the OIPC at their discretion.

Discussion
Developments in information technology create new opportunities for public bodies to collect, use and disclosure personal information more efficiently. However, these same developments also introduce new risks to the security of that personal information.

Privacy breaches pose harm to individuals by creating risks such as identity theft, damage to reputation and relationships, or loss of employment, business, of professional opportunities. They also undermine overall confidence in how public bodies manage personal information, whether it is a lost hard drive containing personal information, health authority staff snooping in electronic health records, or a malicious attack on a public body's information system.

FIPPA applies to all personal information — including health information — which makes it all the more important to require breach notification and reporting. Other jurisdictions in Canada have privacy laws that are specific to health information. Recognizing the sensitivity of health information, most of those statutes require mandatory reporting of significant breaches.[35]

Through recent OIPC audits of privacy breach practices in government and across health authorities, we estimate that only one percent of breaches that occur in government bodies and less than one percent of breaches that have occurred across health authorities over the last 10 years are reported to the OIPC.[36] This statistic is unsettling because discussions with my Office can, in many cases, assist in minimizing the harms that breaches can cause and help to put breach management practices in place that will ultimately reduce the incidents of breaches going forward.

In addition, having a specific requirement spelled out in legislation would provide a standard for public bodies to follow when considering whether to notify

---

[35] See *Personal Health Information Protection Act*, 2004, ON Reg. 329/04; *Personal Health Information Privacy and Access Act*, SNB 2009, c. P-7.05; *Personal Health Information Act*, SNS 2010, c. 41; *Personal Health Information Act*, SNL 2008 CHAPTER P-7.01; *Health Information Act*, SNWT, 2014, c. 2; and PEI and the Yukon have Bills that have received Royal Assent and are not yet in force.

[36] OIPC BC, *Examination of British Columbia Health Authority Privacy Breach Management*, September 30, 2015, at: https://www.oipc.bc.ca/special-reports/1864.

individuals of a breach. This would bring clarity that currently does not exist for public bodies about when to notify.[37] More importantly, it would ensure that individuals can be confident that they are receiving the information needed to take steps to protect themselves to mitigate further harm.

Privacy breaches are particularly troubling in the public sector because government bodies collect large volumes of sensitive personal information. This includes tax information, files about children in care, social assistance data, and law enforcement information. Moreover, as consent is generally not a requirement for collection under FIPPA, citizens often have little choice but to hand personal information over and trust that public bodies with manage it appropriately.

In 2015, the OIPC conducted audits of privacy breach management by the Government of B.C. and eight Health Authorities,[38] the findings of which strongly support the need for breach notification and reporting in British Columbia.

The audits identified some fundamental gaps in breach management within health authorities. For example, only half of the health authorities audited had policies in place for the timing of notifications to individuals, and, as noted above, less than one percent of breaches are reported to our office. Similarly, our audit of government breach reporting found that in those instances where government notified individuals of a breach, notification occurred between 7 and 39 days after the breach. These delays are not acceptable, as the purpose of providing notification is to mitigate potential harm – including identity theft, financial loss or reputational harm. As such, notice should occur without unreasonable delay after a breach is discovered.

FIPPA requires public bodies to be responsible for protecting personal information against such risks as loss or unauthorized access, collection, use, disclosure, or disposal.[39] Every public body should have breach protocols in place to uphold this responsibility. Breach notification and reporting should be an explicit requirement under FIPPA when a privacy breach occurs, because it supports individuals in taking measures to mitigate the harm that can arise from a breach, provides clarity about when to notify and report, and reduces the incidents of breaches going forward.

---

[37] This lack of clarity is discussed in OIPC BC, *An Examination of BC Government's Privacy Breach Management*, January 28, 2015, at: https://www.oipc.bc.ca/special-reports/1749, at pp. 26 and 27.

[38] See OIPC, "*Examination of British Columbia Health Authority Privacy Breach Management*", September 30th, 2015, at https://www.oipc.bc.ca/special-reports/1864 and OIPC, "*Examination of BC Government's Privacy Breach Management*", January 28, 2015, at: https://www.oipc.bc.ca/special-reports/1749.

[39] Section 30.

Mandatory public sector breach notification and reporting exists in Newfoundland and Labrador, in Nunavut, and in seven health privacy statutes in Canada, and by policy for federal departments and agencies.[40] In Europe, it is part of the draft EU General Data Protection Regulation, which, if passed as expected in 2016, will create mandatory breach notification and reporting across all countries in the EU.[41]

Conclusion
FIPPA should include a breach notification and reporting regime that contains a number of key components.

Those components should include the definition of a breach and a duty for the public body to notify affected individuals, and to report to the OIPC "without unreasonable delay" when a significant breach is discovered or suspected. This would place the onus on the public body to explain to the OIPC any delays in notification and reporting, and why they are reasonable.

Individuals should be notified when their personal information is affected by a known or suspected breach, if the breach could reasonably be expected to cause significant harm to the individual.

Public bodies should be required to report to the Commissioner, if a breach could reasonably be expected to cause harm to the individual and/or if it involves a large number of individuals.

These thresholds take into consideration the volume and sensitive nature of information that public bodies hold. Therefore, it will not be necessary for all breaches to be reported. In other words, breaches that do not create a risk of significant harm would not trigger the duty to notify individuals or report to the Commissioner.

---

[40] *Access to Information and Protection of Privacy Act*, SNL 2015, Ch. A-1.2, s. 64; *Access to Information and Protection of Privacy Act*, SNWT (Nu) 1994, c. 20, s. 49.9 and 49.10; *Personal Health Information Protection Act*, 2004, ON Reg. 329/04; *Personal Health Information Privacy and Access Act*, SNB 2009, c. P-7.05; *Personal Health Information Act*, SNS 2010, c. 41; *Personal Health Information Act*, SNL 2008 CHAPTER P-7.01; *Health Information Act*, SNWT, 2014,c. 2; PEI and the Yukon have bills that have received Royal Assent and are not yet in force; and see the Treasury Board of Canada Secretariat, "Guidelines for Privacy Breaches", para. 4, at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154.

[41] See Amendment 45 of the draft text amended by the European Parliament, based on the text proposed by the Commission, which states: "as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and …[t]he individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions". European Parliament, *Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, 2012/0011(COD), at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

In cases where the Commissioner is made aware of a breach, but individuals have not been notified, the Commissioner should have the authority to order a public body to notify individuals affected by a breach. Public bodies should also be required to document breaches, including any decision surrounding why an individual was or was not notified, and the OIPC was or was not advised of the breach.

Adding this requirement will ensure affected individuals are aware that their data has been compromised. Reporting the breach to the Commissioner will ensure independent oversight of the public body's management of the breach and to ensure that steps are being taken to mitigate the chances of recurrence.

Recommendation 8:

Add to Part 3 of FIPPA a breach notification and reporting framework which includes:

- **A definition of a privacy breach: includes the loss of, unauthorized access to or unauthorized collection, use, disclosure or disposal of personal information;**
- **A requirement to notify individuals when their personal information is affected by a known or suspected breach, if the breach could reasonably be expected to cause significant harm to the individual;**
- **A requirement that a public body report to the Commissioner any breach involving personal information under the custody or control of that public body, if the breach or suspected breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals;**
- **A timing requirement that process of notification and reporting must begin without unreasonable delay once a breach is discovered;**
- **Authority for the Commissioner to order notification to an individual affected by a breach; and**
- **A requirement that public bodies document privacy breaches and decisions about notification and reporting.**

➢ Require that Disclosures for Planning and Evaluation be De-identified

Issue
In 2011, FIPPA was amended to permit the disclosure of personal information, if it is necessary for the purposes of *planning or evaluating a program or activity of a public body.* However, this amendment was made without the requirement that the information be de-identified. As is, this potentially creates unnecessary privacy risks for the individuals whose personal information is used.

Discussion
In 2010, government asked the Special Committee for an amendment to FIPPA that would permit the disclosure of personal information for the purposes of program planning and evaluation.

The Committee supported government in this recommendation, but also recognized that privacy concerns and risks were associated with permitting disclosures without consent for such broad purposes. The Committee stated that such activities should only happen with de-identified data:

> Amend the Act to include language confirming a broader approach to research so that applied research into issues, facts, trends, etc. for the purpose of program planning and/or evaluation can be undertaken, provided that only de-identified data are used.[42]

FIPPA already contains a similar safeguard in its provisions that permit disclosure for research or statistical purposes.[43] In that case, identifiers must be removed at the earliest possible time.

It is not clear why the government failed to include the de-identification requirement when it amended FIPPA to authorize disclosure for planning and evaluation purposes.

Conclusion
The authorization to disclose personal information inside Canada, if it is necessary for the purposes of planning or evaluating a program or activity of a public body, should include a requirement that the personal information be de-identified at the earliest possible opportunity.

---

[42] Recommendation 21, "Report", Special Committee to Review the *Freedom of Information and Protection of Privacy Act*, 2nd Session, 39th Parliament, May 2010.
[43] FIPPA s. 35.

Recommendation 9:

Add a de-identification requirement to s. 33.2(l) of FIPPA for any personal information that is disclosed for the purposes of planning or evaluating a program or activity of a public body.

➢ Clarify the Limit of the Exemption for Post-Secondary Teaching Materials and Research Information

Issue
Section 3 of FIPPA exempts teaching materials and research information. The intention was to protect a researcher's individual academic endeavour from an access to information request. However, the broad s. 3 exemption appears to remove research data from the protection of privacy provisions in Part 3 of FIPPA. There is the potential for highly sensitive research data to be compiled, used and disclosed outside of FIPPA's privacy and data security provisions.

Discussion
The language in s. 3(1)(e) states that the "The Act applies to all records". A plain reading of the text suggests that the relevant teaching materials and research information are exempt from *all* parts of the Act.

This section was intended to protect researchers and teaching staff from access to information requests that could impact on their academic freedom or intellectual property, not to shield them from the responsibility of protecting personal information when it is the subject of their research.

Yet, my Office has heard from public bodies that interpret s. 3(1)(e) to mean that Part 3 of the Act does not apply to them, even if research information contains personal information. This view does not represent my expectations, or the privacy interests of the people of B.C.

New technologies provide researchers with the ability to work with larger data sets than ever before, and to share data around the world. The risks to personal information today, therefore, are far greater than in the past, and it is reasonable for people to expect that their personal information, if it is subject to academic research, will be protected.

Previous recommendations
This matter was discussed in some detail by the Special Committee in 1999[44] . The Committee recommended:

> That the FIPPA be amended to apply its privacy provisions to the teaching materials and research information of employees of post-secondary educational bodies, while maintaining their exemption from the access provisions of the Act.[45]

While amendments were subsequently made to this provision, they did not address this issue.

Conclusion
Clarity is needed on the limitations of the s. 3(1)(e) exemption for teaching materials or research information. The application of this section should be limited to Part 2 of FIPPA as was intended, so that the people of B.C. can be assured that their personal information will be protected, if it is used for research purposes at post-secondary institutions.

Recommendation 10:

That FIPPA be amended to limit the exemption in s. 3(1)(e) to Part 2 of FIPPA.

➢ HARMONIZE THE CORRECTION THRESHOLD WITH PIPA

Issue
FIPPA does not clearly set out when public bodies are required to correct personal information. This results in uncertainty for the public.

Discussion
FIPPA requires that public bodies keep information accurate and up-to-date,. Section 29 of FIPPA also contains the right for individuals to request that their personal information be corrected, but does not identify when a public body is required to correct information.

---

[44] See Transcripts of Proceedings (Hansard), Special Committee to Review the *Freedom of Information and Protection of Privacy Act,* 1998/99, Legislative Session: 3rd Session, 36th Parliament, Thursday, July 8, 1999, starting at 0935, at http://www.leg.bc.ca/cmt/36thParl/foi/hansard/fi0708.htm.

[45] Recommendation 2, Report "Special Committee to Review the *Freedom of Information & Protection of Privacy Act*", 3rd Session, 36th Parliament, British Columbia Legislative Assembly, July 15, 1999, at: http://www.leg.bc.ca/cmt/36thParl/foi/1999/review_act.htm.

In contrast, PIPA requires organizations to correct personal information in response to a request to do so when "the organization is satisfied on reasonable grounds that a request made [to correct personal information] should be implemented."[46]

Conclusion
FIPPA should set out a clear threshold at which a public body is required to correct personal information. The threshold should be harmonized with the "reasonable grounds" threshold set out in PIPA. This will promote parity between the Acts and allow for certainty for individuals that a reasonable request to correct information will not simply result in an annotation to a record.

Recommendation 11:

Add to s. 29 of FIPPA a requirement that public bodies correct personal information when an individual requests that his or her personal information be corrected if the public body is satisfied on reasonable grounds that the request made should be implemented.

2.3 Promoting Effective Oversight

Effective independent oversight is necessary to ensure that public bodies carry out the duties and responsibilities that support the purposes of FIPPA.

Independent oversight remains most effective when updates to FIPPA ensure that oversight can be *relevant* and *responsive* to the issues that we face in access and privacy in B.C.. The recommendations in this section promote effective oversight over access to information and privacy rights in B.C..

➢ Create an Offence and Oversight for Unauthorized Destruction of Records

Issue
The unauthorized destruction of records obstructs the rights of British Columbians to access information held by public bodies by removing information from the public record and making it unavailable for access to information requests. It also diminishes the historical record of actions and decisions taken by government.

[46] Section 24(2).

Discussion

When the unauthorized destruction of records occurs, information is destroyed that may otherwise be responsive to a freedom of information request, or may have value for evidence-based decision making or litigation. The public loses forever the ability to access this information, and in fact may not know that the information ever existed. Further, the limited consequences or sanctions for individuals who destroy information have created an incentive to err on the side of destruction rather than preservation.

The unauthorized destruction of records is an area of significant public concern in British Columbia and elsewhere in Canada. Recent incidents in British Columbia, Ontario and Alberta highlight the importance of independent oversight over the destruction of records. The public *must* have the opportunity to understand and to hold public bodies accountable for their actions and decision-making processes. The ability to gain access to records through access to information requests allows for that accountability.[47]

My recent investigation into allegations of the destruction of records identified the deficiencies in access to information practices in two government Ministries and in the Office of the Premier.[48]

Currently, in British Columbia, my Office has narrow authority to investigate the destruction of records. We may only investigate if the alleged destruction of records occurred *after* an access request was made. This lack of oversight runs contrary to the spirit of FIPPA. Effective oversight would permit my Office to investigate *any* complaint concerning the destruction of records – even in the absence of an access request.

Government recently passed the *Information Management Act* (IMA) which, once enacted, will repeal and replace the *Document Disposal Act*. Both Acts deal with the retention and destruction of government records. However, while the

---

[47] In May 2015 the Information and Privacy Commissioner of Alberta is conducting a joint investigation with the Public Interest Commissioner into the allegation of unauthorized destruction of records at the Ministry of Environment and Sustainable Resource Development, see "Joint investigation launched into alleged improper destruction of records by Alberta Environment and Sustainable Resource Development", News Release, May 13, 2015, at: http://www.oipc.ab.ca/pages/NewsReleases/default.aspx?id=4613 ; the Information and Privacy Commissioner of Ontario conducted a special investigation into an allegation that staff at the former Minister of Energy's office inappropriately deleted emails in relation to the cancellation and reallocation of gas plants, see IPC, Deleting Accountability: Record Management Practices of Political Staff - A Special Investigation Report, June 5, 2013, at: https://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=9181.

[48] OIPC BC, Investigation Report F15-03, "Access Denied: Record Retention and Disposal Practices of the Government of British Columbia", October 22, 2015, at: https://www.oipc.bc.ca/investigation-reports/1874.

Document Disposal Act made it an offence to destroy records except as authorized by that Act, the new IAM removes the offence provisions, lowering the consequences for unauthorized destruction of records. In addition, neither statute applies or applied to the broader public sector (*e.g.,* municipalities, school boards and universities).

The Information and Privacy Commissioner of Alberta has the power to investigate compliance with rules in any enactment of Alberta that addresses the destruction of records. Alberta's *Freedom of Information and Protection of Privacy Act* states that the Commissioner has the power to:

> conduct investigations to ensure compliance with any provision of this Act or compliance with rules relating to the destruction of records
> (i) set out in any other enactment of Alberta, or
> (ii) set out in a bylaw, resolution or other legal instrument by which a local public body acts or, if a local public body does not have a bylaw, resolution or other legal instrument setting out rules related to the destruction of records, as authorized by the governing body of a local public body, [49]

In addition, the Alberta statute sets out the unauthorized destruction of records as an offence.[50]

The Ontario legislature also recently passed the *Public Sector and MPP Accountability and Transparency Act*, which amends the freedom of information legislation in Ontario to make the unauthorized destruction of records an offence and provides the Information and Privacy Commissioner with oversight to investigate the issue should it arise.[51]

Conclusion

The unauthorized destruction of records defeats the underlying purpose of the right to access information and can harm accountability. To ensure that records are available to the public, my Office needs to have jurisdiction over the destruction of records, irrespective as to whether an access request is made.

FIPPA should be amended to give my Office oversight over the destruction of records. The amendment should include oversight over destruction in relation to the IMA, any other relevant statutes, and in relation to local public bodies. It

---

[49] Section 53(1)(a) of the Alberta *Freedom of Information and Protection of Privacy Act*.
[50] Section 92(g), *Freedom of Information and Protection of Privacy Act* [RSA 2000].
[51] Bill 8, the *Public Sector and MPP Accountability and Transparency Act* amended *the Freedom of Information and Protection of Privacy Act* to make it an offence to "alter, conceal, or destroy a record, or cause any other person to do so, with the intention of denying a right under this Act to access the record or the information contained in the record". The Bill gained Royal Assent in December 2014 and is online at: http://www.ontla.on.ca/web/bills/bills_detail.do?locale=en&BillID=3000&detailPage=bills_detail_the_bill.

should also be accompanied by appropriate sanctions. This would send a clear signal to public bodies that the unauthorized destruction of records is prohibited in B.C..

Recommendation 12:

Amend s. 42 of FIPPA to expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records.

The Commissioner should have jurisdiction over the unauthorized destruction of records as set out in:

- **any enactment of British Columbia, or**
- **set out in a bylaw, resolution or other legal instrument by which a local public body acts or, if a local public body does not have a bylaw, resolution or other legal instrument setting out rules related to the destruction of records, as authorized by the governing body of a local public body.**

The oversight over unauthorized destruction should come with complementary offences and penalties under FIPPA.

➢ Broaden the Definition of Data-Linking for the Purpose of Oversight

Issue

Data-linking is the matching of personal information from various sources in order to find linkages in information. However, the definition of "data-linking" in the legislation has been interpreted to apply more narrowly than was originally intended or envisioned. Instead of capturing most data-linking initiatives, the definition captures few as it only applies to circumstance where *both* of the databases are being linked for purposes different from those that they were collected for. The result is that very few data-linking initiatives are subject to review by my Office—a review which was intended by government to mitigate privacy risks.

Amendments to FIPPA in 2011 required public bodies to provide early notice and privacy impact assessments for data-linking initiatives for the Commissioner's review and comment. The amendments also authorized the Lieutenant Governor in Council to make regulations respecting how data-linking initiatives must be carried out, after consultation with the Commissioner.

Discussion
When personal information is compared during data-linking, the objective may be to make decisions about the individuals whose personal information is being linked. Data-linking programs may result in decisions to take adverse actions against individuals, for example, the denial of a benefit.

Data-linking raises privacy risks because it:

- may involve the use of data for purposes other than those for which it has been supplied or obtained. (A basic privacy principle is that personal information should be used only for the purpose for which it was obtained. Departures from this principle need to be justified on strong public interest grounds);

- can involve the automatic examination of the personal information of many thousands of people about whom there are no known grounds for suspicion and where no action is warranted;

- relies on public bodies gaining access to large amounts of information, some of which may be personal information, from other sources. There is the potential for public bodies to keep unlinked information even though it has no immediate application or it is no longer necessary; and

- may not be reliable. A data-linking program may fail to distinguish between individuals with similar personal details; input data may be faulty; errors may be made in programming; or difficulties may be caused where similar fields in different databases are not precisely comparable.

Independent review of data-linking is necessary because it takes place without transparency, and without the knowledge of those being scrutinized.

Previous recommendations
Our office made two recommendations related to "data-sharing" in our submission to the 2010 Review Committee:

- Government should not proceed with any more data sharing initiatives until a meaningful public consultation process has occurred, and the outcome of that process is an enforceable code of practice for data sharing programs; and
- FIPPA should be amended to give the OIPC a statutory mandate to review and approve all data-sharing initiatives.

In response to these recommendations, the 2010 Committee only recommended that government "consider holding public consultations on data-sharing

initiatives." While in 2010 my Office used the term "data-sharing" to refer to this type of disclosure and data-matching between public bodies, the Legislature used the term data-linking in the 2011 FIPPA amendments. The terms are referring to the similar activities.

Conclusion
The definition of data-linking that was added to FIPPA in 2011 was drafted in language that was too narrow to capture most, if not all, data-linking initiatives. Therefore, my Office and the public have little knowledge of what data-linking is taking place. No privacy impact assessments have been submitted for review, and no regulations ensure these activities are being undertaken in a responsible manner.

The definition of data-linking should be broadened to encompass more activities and ensure that the original policy objectives underlying the data-linking provisions in FIPPA are met. This will ensure that appropriate activities are subject to independent oversight.

The current definition of data-linking only captures circumstances where the purpose for the data-linking is different from the original purpose of each of the databases being linked. In order for a program to be "data-linking," and subject to review, *each* data set being linked must have been originally obtained or compiled for a purpose that is different from the purpose of the linking.

This means, for example, government could run auto accident records against mental health records to determine whether there is a correlation between health status and automobile accidents. In this hypothetical example, ICBC would be linking the information for a consistent purpose — to track accident rates and set risk-based insurance rates. Only the health information is being linked for a new purpose which means that there would be no notice or privacy impact assessment required. Yet individuals do not expect that their mental health information will be shared with ICBC. As such, data-linking initiatives should be subject to the oversight of my Office to ensure that privacy considerations are accounted for.

In order to encompass a wider range of programs, the definition for data-linking should be broadened to include *any* initiative where the purpose of linking or combining the information is different from the original purpose for which the information in *at least one* of the data sets was originally obtained or compiled.

The change from "each" to "at least one" means that any program that is using a database that was not collected for the purpose of the linking would be considered data-linking under FIPPA, and this re-purposing of personal information would be subject to the oversight of my Office.

Government and my Office are in agreement that the current definition does not provide for adequate oversight of data-linking. We also agree on the amendment to the definition that would ensure that data-linking is subject to adequate review by the OIPC.

Recommendation 13:

Amend the definition for "data-linking" in Schedule 1 of FIPPA to define data-linking as the linking or combining of data sets where the purpose of linking or combining the information is different from the original purpose for which the information in at least one of the data sets that was originally obtained or compiled, and any purposes consistent with that original purpose.

➢ INCLUDE HEALTH INFORMATION IN THE DEFINITION OF DATA-LINKING

Issue
Data-linking activities that are carried out in the health sector were "carved out" of the provisions in FIPPA that provide for independent oversight of data-linking by my Office. The highly sensitive health information of British Columbians is at risk because it is not accorded the same privacy protective oversight measures as data-linking that is carried out by non-health care public bodies.

Discussion
When additional oversight over data-linking initiatives was added to FIPPA in 2011, a special "carve-out" exempted data-linking initiatives carried out by a health care body, the Ministry of Health or a health-related organization. The exemption, however, also removed privacy protections for the personal health information used by these bodies. This is some of the most sensitive information in the custody or control of any public body. It can relate to physical and mental health conditions, health outcomes and laboratory test results, which may carry stigma for the individuals involved.

Further, the personal information held by the Ministry of Health is not limited to personal health information; it also includes financial information collected to establish eligibility for benefits such as PharmaCare and Medical Services Plan.

When it enacted the data-linking provisions in 2011, government stated its concern that the application of those provisions to the health sector may have unintended consequences which could affect the effectiveness, delivery and quality of health care. At that time government committed to me and in the Legislature to work with my Office to address the privacy risks associated with this carve-out. Those limited discussions have, now four years later, not led to

any action by government to resolve my concerns in relation to data-linking in the health sector.

Conclusion
Data-linking in the health sector should not be exempt from independent oversight.

The security and privacy of British Columbians' personal health information should be subject to the same level of privacy protection as other types of personal information.

Recommendation 14:

Repeal s. 36.1(2) of FIPPA to remove the exemption of the health care sector from the data-linking oversight provisions of the Act.

➢ INCREASE THE PENALTIES FOR INDIVIDUALS CONVICTED OF AN OFFENCE

Issue
Penalties are an important incentive for compliance when they are built into any statute. However, the penalties in FIPPA for an individual who commits an offence are amongst the lowest in the country. This is particularly problematic, given the adoption of new digital technologies.

Discussion
Public bodies, including government ministries, are using electronic systems that are increasingly integrated. The public expects that these systems will be accessed by trusted individuals who will handle their personal information in a confidential and secure manner. Unfortunately, there are many cases where individuals abuse their access privileges for their own purposes.

In British Columbia, we have had seen instances of inappropriate disclosures of patient information by health care providers through social media, including posting images or comments about patients on Facebook, Instagram or Twitter.[52] This kind of behaviour is one of the most offensive privacy violations because it violates patient trust in such a public way.

---

[52] For a discussion by the Information and Privacy Commissioner for BC about the privacy issues raised when health care providers engage in snooping and/or the deliberate disclosure of personal health information using mobile devices and social media in health care see OIPC, "Examination of British Columbia Health Authority Privacy Breach Management", September 30th, 2015, at https://www.oipc.bc.ca/special-reports/1864, at pp. 16 and 21.

Currently, FIPPA contains two types of penalties: those for general offences, and those for privacy protection offences.

For **general offences** under FIPPA, any person who commits an offence is liable to a fine of up to $5,000. It is a general offence under FIPPA to willfully:

> (a) make a false statement to, or mislead or attempt to mislead, the commissioner or another person in the performance of the duties, powers or functions of the commissioner or other person under this Act;
>
> (b) obstruct the commissioner or another person in the performance of the duties, powers or functions of the commissioner or other person under this Act;
>
> (c) fail to comply with an order made by the commissioner under section 54.1 or 58 or by an adjudicator under section 65 (2).[53]

For **privacy protection offences** under FIPPA, any person who commits a privacy protection offence is liable to a fine of up to $2,000.

The privacy protection offences under FIPPA prohibit any disclosure of personal information that is not authorized under FIPPA. They also require notification to the head of a public body when any unauthorized disclosures of personal information occur.[54]

In contrast to these penalties under FIPPA, other statutes across the country contain higher penalties — and in many cases, significantly higher penalties — for similar offences.

The Ontario government recently tabled a bill that will increase penalties to up to $100,000 for individuals and to up to $500,000 for corporations and other entities for similar general offences under its *Personal Health Information Protection Act*.[55] The increase was reportedly[56] to deter snooping into health records.

---

[53] See s. 74(1).

[54] Section 74.1(1). Section 74.1, paras. (2) and (3) also include offences for service providers, or an employee or associate of a service provider, to store or access personal information outside of Canada in contravention of the requirements in s. 30.1. They also make it an offence under the Act to contravene other sections that were brought in with s. 30.1, such as the obligation to report foreign demand for disclosure and whistle-blower protection. However, other jurisdictions in Canada do not contain requirements similar to those in s. 30.1 (other than Nova Scotia) so comparative information on penalty amount from multiple jurisdictions is not available.

[55] See s. 2(5) of Bill 119, *Health Information Protection Act, 2015*, at http://www.ontla.on.ca/web/bills/bills_detail.do?locale=en&Intranet=&BillID=3438 for changes in penalties to offences under ss. 72(1)(g), (h) and (i) of the *Personal Health Information Protection Act* [S.O. 2004], at http://www.ontario.ca/laws/statute/04p03#BK93. The Bill will increase the penalties from up to $50,000 to up to $100,000 for natural persons, and from up to $250,000 to up to $500,000 for non-natural persons.

A number of other provinces also have tougher penalties for individuals who have committed similar offences. Penalties are up to $50,000 in Alberta's *Health Information Act*, Saskatchewan's *Health Information Protection Act*, and both Manitoba's *Freedom of Information and Protection of Privacy Act* and its *Personal Health Information Act*. Penalties are up to $25,000 in the Yukon's *Health Information Privacy and Management Act* and up to $10,000 in Alberta's *Freedom of Information and Protection of Privacy Act*, PEI's *Freedom of information and Protection of Privacy Act*, and Newfoundland and Labrador's *Access to Information and Protection of Privacy Act* and its *Personal Health Information Act*.[57]

Conclusion

British Columbia has some of the weakest penalties in Canada for individuals who commit offences under public sector privacy law. This undermines the role that penalties play as an incentive for compliance, suggesting that the government does not take access and privacy seriously.

Penalties under FIPPA should be raised given the sensitivity of the personal information that public bodies hold under FIPPA and the integrated information management systems that exist today. Penalties for all privacy offences should be sufficient to assure the public that privacy is taken seriously by all public bodies.

Recommendation 15:

Penalties for offences committed by individuals under FIPPA should be raised to be up to a maximum of $50,000 for both general and privacy offences.

---

[56] Olivia Carville, "New health legislation will improve transparency", *thestar.com*, September 19, 2015, at: http://www.thestar.com/life/health_wellness/2015/09/19/new-health-legislation-will-improve-transparency.html.

[57] See: the *Health Information Act*, RSA 2000, c. H-5, s.107; the *Health Information Protection Act*, SS 1999, c. H-0.021, s. 64; the *Freedom of information and Protection of Privacy Act*, SM 1997, c. 50, s. 85; the *Personal Health Information Act*, SM 1997, c. 51, s. 64; the *Health Information Privacy and Management Act*, SY 2013, c. 16, s. 122; the *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25, s. 92; the *Freedom of information and Protection of Privacy Act*, RSPEI 1998, c. F-15.01, s. 75; the *Access to Information and Protection of Privacy Act*, SNL 2015, c. A-1.2, s.115; and the *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 88.

➢ CREATE AN OFFENCE FOR UNAUTHORIZED COLLECTION OR USE OF PERSONAL INFORMATION

Issue
FIPPA contains an offence for the unauthorized disclosure of personal information. However, unlike most other provinces, B.C.'s legislation does not impose a general penalty for unauthorized *collection* or *use* of personal information, for instance, for individuals who abuse their access privileges and "snoop" into records.

Discussion
Snooping is the act of intentionally viewing personal information for one's own purpose, whether out of curiosity, concern or for personal gain, in a database that an individual has a right to legitimately access. The subjects of snooping can be family members, colleagues, neighbours, an ex-spouse or partner or a high profile individual.

A serious abuse of privileged access to personal information, snooping can have devastating consequences for individuals such as stigmatization, discrimination and harm. It can also frustrate the systems that public bodies put in place to serve the public. For example, in the context of a health care system, snooping results in a serious breach of trust. This in turn may give patients reservations about sharing personal information or it may alienate them from seeking care.

Offences provide an important incentive for compliance under any statute, including FIPPA.

Most public sector privacy legislation across Canada contains a general offence for *collection*, *use*, *or disclosure* in contravention of the respective statute.[58] In addition many health information acts contain an offence for the same, and some specify an offence for unauthorized access.[59]

B.C. is falling behind other jurisdictions on this issue — not only do other jurisdictions have relevant offences and penalties in place, but prosecutions have

---

[58] See: the *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25, s. 92(1)(a); the *Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. F-22.01, s. 68(1); the *Right to Information and Protection of Privacy Act*, SNB 2009, c. R-10.6, s. 82(1)(a); the *Freedom of Information and Protection of Privacy Act*, RSPEI 1998, c. F-15.01, s. 75(1)(a); the *Access to Information and Protection of Privacy Act*, SNL 2015, c. A-1.2, s. 115(1); *Access to Information and Protection of Privacy Act*, SNWT (Nu) 1994, c. 20, s. 59(1); *Access to Information and Protection of Privacy Act*, SNWT 1994, c. 20, s. 59(1);

[59] *Health Information Act*, RSA 2000, c H-5, s.107; *Health Information Protection Act*, SS 1999, c. H-0.021, s. 64; *Personal Health Information Act*, SM 1997, c. 51, s. 64; *Health Information Privacy and Management Act*, SY 2013, c. 16, s. 122; *Access to Information and Protection of Privacy Act*, SNL 2015, c. A-1.2, s.115; and the *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 88.

begun. For example, Ontario started prosecuting people in 2013 when a nurse at North Bay Regional Health Center was charged with wilfully collecting, using or disclosing the health information of patients in 48 instances in a manner not authorized by Ontario's P*ersonal Health Information Protection Act.*[60] More recently, three hospital workers in Ontario were prosecuted for snooping into the health information of former Toronto Mayor Rob Ford.[61]

Conclusion
While it is an offence to *disclose* personal information in an unauthorized manner, most British Columbians would be surprised to learn that it is not an offence to improperly *access* or *use* personal information.

FIPPA should contain a privacy protection offence for the unauthorized *collection, use, and disclosure* of personal information. This would assure that public that sanctions are available for improper access to personal information in any electronic database system held by a public body.

Recommendation 16:

Add a privacy protection offence to s. 74.1 that makes it an offence to collect, use, or disclosure personal information in contravention of Part 3 of FIPPA.

➢ CONSOLIDATE AND REVIEW OTHER STATUTES THAT PREVAIL OVER FIPPA

Issue
At least 43 B.C. statutes have provisions that override or prevail over FIPPA in whole or in part. However, FIPPA contains no mechanism to review, update or remove them. The rise of these provisions has weakened access to information rights and protection of privacy in B.C., to the detriment of public accountability.

Discussion
I am concerned about the proliferation of provisions which prevail over FIPPA that have been enacted in the last few years.

---

[60] *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A, s. 72. See Maria Calabrese, "Hospital Ordered to Disclose Records", *North Bay Nugget*, July 2013, at: http://www.nugget.ca/2013/07/05/hospital-ordered-to-disclose-record.

[61] Olivia Carville, "Govt. prosecutes health workers for snooping into Rob Ford's medical records", *thestar.com*, July 8, 2015, at: http://www.thestar.com/life/health_wellness/2015/07/08/govt-prosecutes-health-workers-for-snooping-into-rob-fords-medical-records.html.

Section 70 of FIPPA clearly states that where there is a conflict between FIPPA and any other provincial statute, FIPPA prevails unless the other statute expressly states that it overrides FIPPA. This is a clear indication that the Legislature intended the access to information and protection of privacy provisions in FIPPA to take precedence over other statutes, except in extraordinary or unique circumstances.

Freedom of information is a fundamental right, reflected in the fact that individuals can exercise their right to request records from any public body under FIPPA. At its heart, the access to information system supports the notion that the information held by public officials is being held *for the benefit of the public*. We should carefully safeguard this right. FIPPA is balanced to reflect the public's right to access information and the need for public bodies to keep some of that information confidential. Each express FIPPA override that is enacted weakens that balance.

Part 2 of FIPPA already contains 12 exceptions to access which comprehensively provide confidentiality for public bodies and third parties, yet to date government has drafted 43 additional provisions in other statutes that override FIPPA (see Appendix 1).

Newfoundland has added to its access to information legislation a requirement that statutes that prevail over that legislation should be listed in a schedule to that statute and routinely reviewed with it.[62] This approach provides a mechanism for regular reviews of statutory overrides and should be adopted in B.C.

Conclusion

Growth in the list of provisions in statutes that prevail over FIPPA diminishes the access rights of individuals in B.C. Given the fundamental nature of these rights, FIPPA should contain a mechanism for the routine review of these provisions and their impact on freedom of information and protection of privacy. These prevailing provisions should be regularly reviewed alongside this Committee's review of FIPPA to ensure that these exceptions continue to be justified and necessary from a public interest perspective. This review should determine whether the need for a provision has changed over time and whether it continues to serve its intended policy purpose. It could also identify instances where the purpose of the override is already provided for within the 12 exceptions to access already present in FIPPA.[63]

---

[62] Sections 7 and 117.

[63] For example, the *Pharmaceutical Services Act* grants the Minister discretionary authorization to "refuse to make public information respecting the deliberations and recommendations, by an advisory committee or by employees of the ministry of the minister" certain information relating to a drug formulary. However, s. 13 of FIPPA already provides this discretionary authorization under the exception for policy advice or recommendations.

Recommendation 17:

Amend Part 6 of FIPPA to require government to list provisions in statutes that prevail over FIPPA in a schedule to the Act, and amend s. 80 of FIPPA to include a review of those provisions as part of the statutory review of the Act.

➢ HARMONIZE SECTION 56 OF FIPPA WITH PIPA.

Issue
Section 56(6) of FIPPA requires that an inquiry into a matter under review must be completed within 90 days after receiving the request for review. FIPPA is silent about the ability of the Commissioner to extend this time period. When a request requires more than 90 days to complete, staff spend considerable time arranging for time extensions with the involved parties. This leads to inefficiencies in an already heavy work schedule.

Discussion
In 2014, my Office completed 620 "requests for review" files. We found that these requests can be resolved more efficiently in mediation, where they are resolved 94% of the time. However, many requests require more than 90 days to complete.

Mediation facilitates a settlement of the issues and ensures that the applicant has received access to all records or information to which he or she is entitled. If mediation is not successful, the Commissioner may hold a formal inquiry.

Under s. 50(8) of PIPA, the Commissioner is granted the authority to extend the time limit for completing reviews. It states:

> An inquiry respecting a review must be completed within 90 days of the day on which the request is delivered under section 47(1), unless the commissioner
>
> (a) specifies a later date, and
> (b) notifies
> i. the individual who made the request,
> ii. the organization concerned, and
> iii. any person given a copy of the request.

Previous recommendations
The Commissioner made this recommendation in the 2004 and 2010 submissions to the Special Committee. In its 2010 report, the Committee wrote that: "The Special Committee agrees that the Commissioner should be permitted

to extend this time limit, for practical reasons and in the interests of consistency with the private sector privacy law."

The Ministry of Technology, Innovation and Citizens' Services has indicated that they generally support harmonizing the public and private sector legislation. However, this recommendation remains unimplemented.

Conclusion
Providing the Commissioner with the ability to extend the 90 day time limit would make FIPPA consistent with PIPA, save the office time and resources currently used to negotiate extensions, and give applicants a better indication of when they can expect their reviews to be complete. The Commissioner should be able to extend the 90 day timeline to review requests as she is able to do under PIPA.

Recommendation 18:

Amend s. 56 of FIPPA to permit the Commissioner to extend the 90 day time limit to review requests in a manner that is consistent with s. 50(8) of PIPA.

➢ COMBINE THE COMPLAINT, REVIEW, AND INQUIRY PROCESSES

Issue
FIPPA provides for two types of public appeals to the OIPC: "complaints" and "requests for review." The distinction between the two is often unclear to the involved parties. This creates confusion and an unnecessary administrative burden.

Discussion
Under FIPPA, a person may file a complaint with the office that a public body is in contravention of the Act (pursuant to s. 42(2)), or they can request that the Commissioner review the outcome of a request made to a public body (pursuant to s. 52(1)). Requests for review can also include any matter that could be the subject of a complaint under s. 42(2). Both types of appeal may, depending on the circumstances, continue on to an inquiry.

FIPPA's process distinction for complaints and requests for review is unnecessary; it is confusing for those involved in these processes and staff spend administrative resources assisting individuals to navigate them.

Previous recommendations
The recommendation to create a unitary process in FIPPA for complaints and requests for review was made by my Office to the Special Committees in 2010 and 2004.[64] Both of the Special Committees to Review FIPPA in 2010 and 2004 included this recommendation in their reports.[65] However, this recommendation remains outstanding.

Conclusion
All parties involved in processes in my Office would benefit from an amendment to harmonize the complaint, review, and inquiry process under FIPPA.

Recommendation 19:

Amend Parts 4 and 5 of FIPPA to combine the complaint process and the review and inquiry process into a unitary process for the Commissioner to investigate, review, mediate, inquire into and make orders about complaints respecting decisions under FIPPA or other allegations of non-compliance with FIPPA.

2.4 Health Information

➢ ENACT A COMPREHENSIVE HEALTH INFORMATION PRIVACY LAW

Issue
Health information is amongst our most sensitive personal information. Yet in British Columbia individuals, health care professionals, and researchers must navigate a patchwork of legislative regimes when it come to the management of health information. This is administratively inefficient for the health sector, is unnecessarily cumbersome for researchers, and ultimately puts the privacy of individuals at potential risk of harm.

---

[64] Recommendation 18, OIPC, "Submission of the A/Information and Privacy Commissioner to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*", March 15, 2010, at: https://www.oipc.bc.ca/special-reports/1275; and Recommendation 25, OIPC, "Submission of the Information and Privacy Commissioner to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*", February 5, 2004, at: https://www.oipc.bc.ca/special-reports/1274.

[65] Recommendation 30, "Report", Special Committee to Review the *Freedom of Information and Protection of Privacy Act*, 2nd Session, 39th Parliament, May 2010; Recommendation 20, "Enhancing the Provinces Public Sector Access of Privacy Law", Special Committee to Review the *Freedom of Information and Protection of Privacy Act*", 5th Session, 37th Parliament, May 2004.

Discussion
This review of FIPPA arrives at a time when there is an urgent need to move the discussion about a health information statute in B.C. from talk into action.

Like many sectors, the health sector has been transformed by new digital technologies. There are new ways of managing health information that create welcome conveniences and opportunities. We see health care providers using tablets for patient files, patient information can be transferred between two points in an instant, and research that would not have been possible when FIPPA was first enacted can and is being done to improve both the health care system and patient care.

These new methods for managing health information must be accompanied by robust privacy protections. Yet in B.C., those protections are spread across a number of statutes. A list of the key pieces of legislation that make up this patch work, and their relevance to access and privacy relating to health information, is set out in Appendix 2. It includes FIPPA for the public sector, PIPA for the Private Sector, and the *E-Health (Personal Health Information Access and Protection of Privacy) Act* which provides a framework that governs privacy and access for electronic health information databases.

The access and privacy safeguards across these statutes have emerged and overlapped over time resulting in a patchwork of regulation that patients, health care providers, and researchers must navigate on a daily basis. I submit that this patchwork results in staff time spent navigating the various statutes and regulations that could be better used in providing direct health services.

B.C. has fallen behind most provinces and territories in Canada, most of which have established health information acts that apply one framework across the private and public sectors.[66] The key recommendation in my special report, *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector*, was that the government enact a new comprehensive health information privacy law at the earliest opportunity. That report set-out the major components for such a law in detail.

That said, the present task is to make recommendations for improvements to FIPPA and many of the recommendations in this submission would enhance the protection of health information held by the public sector in B.C.

---

[66] See: *Health Information Act*, RSA 2000, c. H-5; The *Health Information Protection Act*, SS 1999, c H-0.021; *Personal Health Information Act*, CCSM c. P33.5; *Personal Health Information Protection Act*, 2004, SO 2004, c. 3, Sch A; *Personal Health Information Privacy and Access Act*, SNB 2009, c. P-7.05; *Personal Health Information Act*, SNS 2010, c. 41; *Personal Health Information Act*, SNL 2008, c. P-7.01; *Health Information Act*, SNWT, 2014,c. 2; and PEI and the Yukon have Bills that have received Royal Assent and are not yet in force

Chief amongst these are a statutory requirement for privacy management programs, including breach notification. I made these same recommendations to the Special Committee that conducted the latest review of PIPA as well, and given that health care straddles both the public and private sectors, it is important that these responsibilities exist in harmony across both statutes.

I have also recommended that health information should not be carved out of the definition of data-linking. This will ensure that when the health information of people in B.C. is disclosed through a data-linking initiative, those activities will be subject to independent oversight.

In addition, I have recommended that the existing offence for unauthorized disclosure in FIPPA be expanded to include unauthorized collection and use. This will ensure that there is an offence for "snooping" in FIPPA, and establish that snooping—of health information or other personal information—is not an acceptable activity, particularly when it is undertaken by someone who is authorized to have access for legitimate purposes but takes personal advantage of that access. This is complemented by my recommendation to increase to the maximum penalty available for an individual that is convicted of committing an offence under FIPPA.

Conclusion

This report contains a number of recommendations to enhance the protection of privacy for personal information, which includes personal health information.

However, the blended public and private health sectors, combined with the patchwork of statutes that govern health information laws in B.C., make it challenging for health care professionals and administrators to appropriately and confidently utilize the opportunities offered by new technologies, including the benefits for patient care and research.

British Columbians should be able to rest assured that information is shared appropriately between public and private providers, and that sensitive personal health information is robustly safeguarded.

Recommendation 20:

Government should enact new comprehensive health information privacy legislation at the earliest opportunity.

Summary of Recommendations

Recommendation 1:

Add to Part 2 of FIPPA a duty for public bodies to document key actions and decisions based on the definition of "government information" in the *Information Management Act*.

Recommendation 2:

Section 13(1) of FIPPA should be amended to clarify the following:

- **"advice" and "recommendations" are similar and often interchangeably used terms, rather than sweeping and separate concepts;**
- **"advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process;**
- **the "advice" or "recommendations" does not apply to the facts upon which the advice or recommendation is based; and**
- **the "advice" or "recommendations" does not apply to factual, investigative, or background material, for the assessment or analysis of such material, or for professional or technical opinions.**

Recommendation 3:

Amend FIPPA to move paragraph (n) of the definition of "local government body" into the definition of "public body" in Schedule 1, so that entities such as subsidiaries of educational bodies and the BCACP fall within the scope of FIPPA.

Recommendation 4:

Amend ss. 71 and 71.1 of FIPPA to require the publication of any categories of records that are established by the head of a public body or the Minister and made available to the public without an access request. This list should include links to relevant information or records.

Recommendation 5:

Amend FIPPA to require public bodies to ensure that the name and type of applicant is only disclosed to the individual at the public body that receives an access request on behalf of that public body, while providing for limited exceptions where the applicant is requesting their own personal information or where the name of the applicant is necessary to respond to the request.

Recommendation 6:

Add an exception to s. 33.1(1) that states that a public body may disclose personal information inside or outside of Canada, if the information is contained in a non-statutory investigation or fact-finding report commissioned by a public body, where the head of the public body concludes the public interest in disclosure outweighs the privacy interests of any person whose personal information is contained in the report.

Recommendation 7:

Add to FIPPA a requirement that public bodies have a privacy management program that:

- **designates one or more individuals to be responsible for ensuring that the public body complies with FIPPA;**
- **is tailored to the structure, scale, volume, and sensitivity of the personal information collected by the public body;**
- **includes policies and practices that are developed and followed so that the public body can meet its obligations under FIPPA, and makes policies publicly available;**
- **includes privacy training for employees of the public body;**
- **has a process to respond to complaints that may arise respecting the application of FIPPA; and**
- **is regularly monitored and updated.**

Recommendation 8:

Add to Part 3 of FIPPA a breach notification and reporting framework which includes:

- **A definition of a privacy breach: includes the loss of, unauthorized access to or unauthorized collection, use, disclosure or disposal of personal information.**
- **A requirement to notify individuals when their personal information is affected by a known or suspected breach, if the breach could reasonably be expected to cause significant harm to the individual.**
- **A requirement that a public body report to the Commissioner any breach involving personal information under the custody or control of that public body, if the breach or suspected breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals;**
- **A timing requirement that process of notification and reporting must begin without unreasonable delay once a breach is discovered;**
- **Authority for the Commissioner to order notification to an individual affected by a breach; and**
- **A requirement that public bodies document privacy breaches and decisions about notification and reporting.**

Recommendation 9:

Add a de-identification requirement to s. 33.2(l) of FIPPA for any personal information that is disclosed for the purposes of planning or evaluating a program or activity of a public body.

Recommendation 10:

That FIPPA be amended to limit the exemption in s. 3(1)(e) to Part 2 of FIPPA.

Recommendation 11:

Add to s. 29 of FIPPA a requirement that public bodies correct personal information when an individual requests that his or her personal information be corrected if the public body is satisfied on reasonable grounds that the request made should be implemented.

Recommendation 12:

Amend s. 42 of FIPPA to expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records.

The Commissioner should have jurisdiction over the unauthorized destruction of records as set out in:

- **any enactment of British Columbia, or**
- **set out in a bylaw, resolution or other legal instrument by which a local public body acts or, if a local public body does not have a bylaw, resolution or other legal instrument setting out rules related to the destruction of records, as authorized by the governing body of a local public body.**

The oversight over unauthorized destruction should come with complementary offences and penalties under FIPPA.

Recommendation 13:

Amend the definition for "data-linking" in Schedule 1 of FIPPA to define data-linking as the linking or combining of data sets where the purpose of linking or combining the information is different from the original purpose for which the information in at least one of the data sets that was originally obtained or compiled, and any purposes consistent with that original purpose.

Recommendation 14:

Repeal s. 36.1(2) of FIPPA to remove the exemption of the health care sector from the data-linking oversight provisions of the Act.

Recommendation 15:

Penalties for offences committed by individuals under FIPPA should be raised to be up to a maximum of $50,000 for both general and privacy offences.

Recommendation 16:

Add a privacy protection offence to s. 74.1 that makes it an offence to collect, use, or disclosure personal information in contravention of Part 3 of FIPPA.

Recommendation 17:

Amend Part 6 of FIPPA to require government to list provisions in statutes that prevail over FIPPA in a schedule to the Act, and amend s. 80 of FIPPA to include a review of those provisions as part of the statutory review of the Act.

Recommendation 18:

Amend s. 56 of FIPPA to permit the Commissioner to extend the 90 day time limit to review requests in a manner that is consistent with s. 50(8) of PIPA.

Recommendation 19:

Amend parts 4 and 5 of FIPPA to combine the complaint process and the review and inquiry process into a unitary process for the Commissioner to investigate, review, mediate, inquire into and make orders about complaints respecting decisions under FIPPA or other allegations of non-compliance with FIPPA.

Recommendation 20:

Government should enact new comprehensive health information privacy legislation at the earliest opportunity.

Appendix 1

B.C. Statutes with Provisions that Prevail over FIPPA

Legislation (43 statutes in total)	Section(s) with clauses that fully or partially prevail over FIPPA
Administrative Tribunals Act, SBC 2004, CHAPTER 45	61(2) & (3)
Adoption Act, RSBC 1996, CHAPTER 5	70(3), 74
Adult Guardianship Act, RSBC 1996, CHAPTER 6	46(2)
Animal Health Act, SBC 2014, CHAPTER 16	16(2), 60(a)
Architects Act, RSBC 1996, CHAPTER 17	51.2(3)
Child Care BC Act, SBC 2001, CHAPTER 4	8(4)
Child, Family and Community Service Act, RSBC 1996, CHAPTER 46	24(2) & (3), 74, 75, 77, 96
Coroners Act, SBC 2007, CHAPTER 15	64, 66
Criminal Records Review Act, RSBC 1996, CHAPTER 86	6(3) & (4)
E-Health (Personal Health Information Access and Protection of Privacy) Act, SBC 2008, CHAPTER 38	18(1) & (2), 20
Election Act, RSBC 1996, CHAPTER 106	275(7)
Emergency Communications Corporations Act, SBC 1997, CHAPTER 47	9(4)
Employment Standards Act, RSBC 1996, CHAPTER 113	75(2), 101
Evidence Act, RSBC 1996, CHAPTER 124	51(5)-(8)
Family Law Act, SBC 2011, CHAPTER 25	11, 133(4), 243(3) & (4)
Family Maintenance Enforcement Act, RSBC 1996, CHAPTER 127	43(1)(2)
Health Professions Act, RSBC 1996, CHAPTER 183	26.2(1) & (6)
Heritage Conservation Act, RSBC 1996, CHAPTER 187	3(3)
Income Tax Act, RSBC 1996, CHAPTER 215	64(8)
Legal Profession Act, SBC 1998, CHAPTER 9	88(2),(7) & (8)

LEGISLATION (43 STATUTES IN TOTAL)	SECTION(S) WITH CLAUSES THAT FULLY OR PARTIALLY PREVAIL OVER FIPPA
Local Elections Campaign Financing Act, SBC 2014, CHAPTER 18	63(3)
Local Government Act, RSBC 1996, CHAPTER 323	35
Maa-nulth First Nations Final Agreement Act, SBC 2007, CHAPTER 43	14(2)
Mines Act, RSBC 1996, CHAPTER 293	34(8) & (9)
Motor Vehicle Act, RSBC 1996, CHAPTER 318	93.1
Nisga'a Final Agreement Act, 1999, CHAPTER 2	44
Pharmaceutical Services Act, SBC 2012, CHAPTER 22	7, 25
Police Act, 1996] CHAPTER 367	182
Public Guardian and Trustee Act, RSBC 1996, CHAPTER 383	17(3)
Public Health Act, SBC 2008, CHAPTER 28	53
Public Inquiry Act, SBC 2007, CHAPTER 9	26, 28(7)
Recall and Initiative Act, RSBC 1996] CHAPTER 398	168(8)
Representative for Children and Youth Act, SBC 2006, CHAPTER 29	10(4)(b)
Safety Standards Act, SBC 2003, CHAPTER 39	21
School Act, RSBC 1996, CHAPTER 412	11.7
Securities Act, RSBC 1996, CHAPTER 418	148(2)
Statistics Act, RSBC 1996, CHAPTER 439	9(2) & (3)
Teachers Act, SBC 2011, CHAPTER 19	41(1) & (2), 53(9)
Transportation Investment Act, SBC 2002, CHAPTER 65	25(2.2) & (7)
Vancouver Charter, SBC 1953, CHAPTER 55	8.1
Victims of Crime Act, RSBC 1996, CHAPTER 478	7(2)
Workers' Compensation Act, RSBC 1996, CHAPTER 492	156(5)

Appendix 2

Key Pieces of the "Patchwork" of Health Information Laws in B.C.

Continuing Care Act, s. 5
Authorizes the Ministry and a health authority to require a person to provide information respecting the person or the members of the person's family thought necessary for the proper administration of the Act.

E-Health (Personal Health Information Access and Protection of Privacy) Act
Governs the collection, use and disclosure of personal health information through electronic databases of the Ministry and health authorities that have been designated by the Minister as "health information banks". To date, only applied to a repository of lab data that is part of the provincial EHR system.

Freedom of Information and Protection of Privacy Act
Applies to personal information that is in the custody or control of the Ministry, health authorities, agencies, boards and commissions in the health sector (including the Medical Services Commission) and professional regulatory bodies.

Health Act, ss. 9 and 10
The BC Cancer Agency is authorized to collect, use and disclose information for the purpose of medical research.

The health status registry may request that a person provide it with information concerning congenital anomalies, genetic conditions or chronic handicapping conditions of individuals.

Hospital Insurance Act, s. 7
Authorizes the Ministry or a hospital to require a person to provide information respecting the person or the members of the person's family thought necessary for the proper administration of the Act.

Laboratory Services Act
Governs the collection, use and disclosure of personal information by the Ministry in relation to the payment of benefits for laboratory services.

Medicare Protection Act, s. 49
Section 49 provides that individuals must keep matters about beneficiaries and practitioners that come to their knowledge in the course of administering the Act confidential subject to certain exceptions.

Ministry of Health Act, Part 2
Authorizes the collection, use and disclosure of personal information by the Ministry from a public body for a stewardship purpose.

Personal Information Protection Act
Applies to personal information that is in the custody or control of organizations, including private practices of health professionals and private labs.

Pharmaceutical Services Act
Governs the collection, use and disclosure of personal information by the Ministry in relation to the payment of benefits for pharmaceutical services. Additionally, it governs access to and recording of information in prescribed information management technology.

Public Health Act
Part 1, Division 3 sets our purposes for collection, use and disclosure of personal information related to reporting of reporting disease, health hazards and other matters.

Health Act Communicable Disease Regulation
Governs the collection, use and disclosure of personal information related to public health matters, including mandatory reporting of infectious diseases or health hazards.