ABOVE BOARD

A QUARTERLY NEWSLETTER BY THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

VOLUME 09, ISSUE 04 OCTOBER 2017

CONTACT INFORMATION

Office of the Information and Privacy Commissioner
3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8
Tel: (709) 729-6309
Fax: (709) 729-6500
Toll Free in Newfoundland and Labrador: 1-877-729-6309
Email: commissioner@oipc.nl.ca
www.oipc.nl.ca

"The Commissioner's role is to facilitate the effort of a requestor to seek access to information [...] and is effectively an ombudsman or liaison between the citizen and government in attempting to resolve the request by mediation or otherwise if documents or information known to be existing are being withheld in whole or in part for various reasons"
Justice Harrington, NL CA, NL (Information and Privacy Commissioner) v. NL (Attorney General)

OIPC REMINDERS AND UPDATES

OIPC Website Now Searchable

The OIPC website, including Commissioner's Reports, is now searchable. The search field is located at the top of the "Commissioner's Reports" page under the "Reports" menu. Results include .pdf documents such as: Commissioner's Reports, Guidance Documents, presentations, newsletters, and annual reports.

ATIPP Office Guide for Municipalities

Municipal Coordinators are reminded that the ATIPP Office has created the ATIPPA Guide for Municipalities publication which is a very useful tool covering access to public information, privacy issues, and responding to access to information requests.

Need for Effective and Timely Means of Communication with Complainants

The OIPC has placed a notice on its website which requests that, wherever possible, complainants provide email or telephone contact information on complaint forms. The reason for this is due to the strict timelines imposed upon this Office in carrying out its investigations under the *ATIPPA, 2015*. As such, we must have an effective and timely means of communication with complainants. Complainants have been advised that if they are unable to communicate with this Office via email or telephone, we will make every effort to investigate their complaints to the fullest extent, however, matters may be hindered by time constraints.

PROVIDING REASONS FOR REFUSAL OF ACCESS

In accordance with section 17(1)(c), where a public body refuses access to information in response to an access to information request, the public body must inform applicants of the exemptions being relied upon.

A public body is not required to disclose the contents of the records being withheld, but must provide the applicant with more than a recitation of the section being relied upon. The public body should indicate: why the specific exception applies to the withheld information; which element(s) of the exception are relevant; and why, with reasonable detail, those elements apply to the requested information.

The requirement to provide reasons also extends to section 40 (disclosure harmful to personal privacy) of the *ATIPPA, 2015*. It is not sufficient for a public body simply to state that the information is an unreasonable invasion of a third party's personal privacy. A public body must provide the applicant with adequate information to understand why the disclosure would be an unreasonable invasion of a third party's privacy. However, a public body must also be cautious not to provide so much detail in its explanation so as to reveal the identity of the third party or any information that is required to be withheld. Reasons should also include a discussion of the public body's consideration of the factors outlined in subsection 40(5), if applicable.

The reasons why a request was refused are an essential part of the response to an applicant. If applicants can clearly understand why access is refused, they may accept the public body's response. Ambiguity as to the reasons for refusing a request leads to a greater likelihood of complaints about the decision to refuse access. Even if a complaint is made, a thorough explanation of the reasons for the refusal can assist in facilitating an informal resolution.

Our full guidance piece can be found on our website.

Sharpening Your Teeth
Advanced Investigative Training for Administrative Watchdogs

On October 10th and 11th, the OIPC, along with the Office of the Advocate for Children and Youth, Elections NL and the Office of the Citizens' Representative attended training from the Office of the Ombudsman Ontario. The training focused on conducting administrative investigations.

(L-R: Bruce Chaulk, Wendy Ray, Jackie Lake-Kavanagh, Laura Pettigrew, Donovan Molloy, Brad Moss)

TRAVELLING WITH MOBILE DEVICES

Canada's Privacy Commissioner, Daniel Therrien has advised that U.S. Customs officers are entitled to look at mobile devices and even demand passwords under American law and unless you are unconcerned about U.S. officers accessing your mobile devices, you should not take them across the U.S. border.

If you are an employee of a public body and/or custodian and you are travelling with a device issued to you by your employer which has **personal information** and/or **personal health information** stored on it (or provides access to same) you have legal obligations to protect the privacy of that information. Border officials may ignore claims of privacy and legal duties pursuant to the *ATIPPA, 2015* and/or *PHIA*. As such, you should carefully consider whether you might be risking exposure of personal information and/or personal health information to foreign government officials when crossing borders and take appropriate steps before travelling.

Public bodies and custodians are legally obliged to ensure that reasonable safeguards are in place to protect the privacy of personal information and/or personal health information. At a minimum, this requires policies regarding travelling while in possession of employer—issued mobile devices. Those policies should prohibit carrying personal information or personal health information on electronic devices while travelling. These policies must be communicated to all employees.

While both the *ATIPPA, 2015* and *PHIA* permit disclosures required by law, it is our position that this is limited to Canadian law and excludes knowingly creating the potential for disclosure of personal information and/or personal health information to foreign government officials.

For employees who use their personal devices to conduct the business of a public body and/or custodian the same considerations apply. Also, policies should cover both work and personal travel of employees. The practice of allowing employees to use their personal devices for business purposes, even with stringent safeguards, carries additional risks of unauthorized disclosure and further complicates crossing the U.S. border.

Our suggestions for measures that should be considered and included in travel policies and procedures and further details are included in the full guidance piece.

PRACTICE TIP

Where practical, identify a back-up coordinator. This person should be kept acquainted with on-going requests and the process under the *ATIPPA, 2015* so that they are able to assist on larger requests, can handle requests where there is a high volume, and can actively engage with this Office and the applicant where the coordinator is unavailable or is in a conflict

USE OF SOCIAL MEDIA – QUICK TIPS

Social media is a term used to describe on-line technologies, applications and practices that are used to share information, knowledge and opinions (e.g. social networking sites, blogs, wikis, content sharing sites, photo sharing sites, and video sharing sites).

In any use of social media, it is paramount that public bodies and custodians properly manage and protect the privacy of personal information. Below are some quick tips on how to use social media while still meeting your statutory responsibilities and obligations.

- Limit who is authorized to post to social media on behalf of a public body or custodian.
- Never collect or disclosure personal information or personal health information via social media.
- Immediately remove personal information and personal health information which is posted contrary to the *ATIPPA, 2015* or *PHIA* and alert your ATIPP Coordinator and the OIPC.
- Only post to social media at the direction of an authorized individual and only after ensuring that the post complies with the relevant policies of your public body or custodian, and all applicable provisions of *ATIPPA, 2015* and *PHIA*.
- Limit the number of platforms used and delete any social media accounts that are inactive or unmoderated.
- Complete a Privacy Impact Assessment.
- Make individuals aware of the platforms you use.
- Familiarize yourself with and ensure to use the privacy settings of the platform.
- Use strong password protection.

For a greater discussion on the use of social media please see the full guidance piece

IMPORTANT NOTICE

Where, through the informal resolution process with the OIPC, the parties are able to reach an agreement for the release of information, coordinators must be mindful to notify the OIPC when the information is released. This is most easily achieved by copying the OIPC on the letter to the complainant enclosing the information.

MINIMUM AMOUNT NECESSARY

The minimum necessary standard is provided for in sections 66(2) and 68(2) of the *ATIPPA, 2015*. Simply put, a public body must collect, use and disclose only as much personal information as is reasonably necessary to accomplish the purpose for which it is permitted to be used or disclosed under sections 66 and 68. Public bodies must review their policies and procedures to ensure that unnecessary collections, uses and disclosures do not occur. If a public body uses or discloses more personal information than is necessary to accomplish an authorized purpose, the public body will not be in compliance with the *ATIPPA, 2015* and may be subject to a privacy complaint, audit or investigation by this Office.

A public body should consider the following before collecting, using or disclosing personal information: the reason for the collection, use or disclosure; whether that purpose is authorized under the *Act;* if it is advisable to obtain consent; and how to limit the collection, use or disclosure to the minimum amount of information necessary to accomplish the authorized purpose (i.e. the "need to know" principle).

Public bodies should develop a public written statement about the uses to which it will put the personal information in its custody and control and when that information can be disclosed.

It is useful for public bodies to keep a record of every disclosure of personal information including a description of the information, who disclosed it, to whom it was disclosed, and the reasons for the disclosure. This way, if an issue is raised, the public body can readily respond to any inquiries.

You can review the full guidance piece on our website

ABIDING BY STATUTORY DEADLINES

We would like to remind coordinators that the *ATIPPA, 2015* imposes firm deadlines for the conduct of an investigation and obliges us to issue a report within 65 business days of receiving a complaint. Paragraph 44(2) states that parties may, not later than 10 business days after receiving notification, make representations. Allowing for extensions to the timeframe for responding to our Office at the outset of an investigation would cut deeply into our deadlines.

Further, in the conduct of an investigation, the first 30 business days are spent in an attempt to resolve a matter informally to the satisfaction of the parties, without requiring further investigation or potentially binding recommendations. If we are unable to resolve the matter within that time, we proceed to a formal investigation which may result in a public report from this Office. A delay by a public body in making its submissions makes it less likely that an informal resolution will be reached.

Public bodies who fail to make their submissions within the 10-day period may miss the only opportunity to make submissions in these matters and, once the informal investigation period ends this Office may be forced to issue a report with recommendations for the public body to follow. It is in the best interests of a public body to make its submissions as soon as possible and within the 10-day deadline if the public body wants its position is to be considered by this Office.

ATIPPA PRIVACY BREACH STATISTICS July 1 - September 30, 2017

During this reporting period (July 1 - September 30, 2017), the OIPC received 45 privacy breach reports from 15 public bodies under the *ATIPPA, 2015*. This is up from the 41 reports from 15 public bodies received in the second quarter of 2017/2018.

If any public body would like the OIPC to deliver training regarding privacy breaches, or any other topic relating to access or privacy, contact our Office to arrange a time.

Summary by Public Body	
Advanced Education, Skills and Labour	1
City of Corner Brook	2
City of St. John's	1
College of the North Atlantic	4
Department of Children, Seniors and Social Development	5
Department of Finance	2
Department of Justice and Public Safety	1
Department of Transportation and Works	1
Eastern Health	5
Human Resource Secretariat	1
Memorial University of Newfoundland	2
Newfoundland and Labrador English School District	4
Newfoundland and Labrador Housing Corporation	1
Service NL	14
Western Integrated Health Authority	1

Summary by Type	
Email	13
Fax	6
In Person	8
Intentional (i.e. willful breach)	1
Mail Out	13
Other	3
Technical Malfuncion	1

The OIPC has issued a tip sheet on Avoiding Inadvertent Privacy Breaches visit our website @

www.oipc.nl.ca