ABOVE BOARD

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

VOLUME 10, ISSUE 02 APRIL 2018

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)

- 2018 APSIM Conference
- Privacy Management Programs
- Designating the Head of a Local Public Body
- The Importance of Auditing Access
- Retention of Records
- Balancing Workload and Statutory Deadlines
- Privacy Training Expectations
- *ATIPPA, 2015* Privacy Breach Statistics Jan. 1 - Mar. 31, 2018

OIPC REMINDERS AND UPDATES

2018 APSIM Conference

The website for the 2018 APSIM Conference, *We are Connected – Control–Alt–Delete: Control Data, Use Alternatives, and Delete Risks"*, is now live: www.gov.nl.ca/apsim.

This year's FREE conference promotes collaboration and builds awareness of the overlap and interplay between the access, privacy, security and information management communities. Our goal is to facilitate our ability to assist each other in managing, protecting and securing information.

Be sure to visit the website to see the conference agenda and find many more conference details, including the event registration link.

If you have any questions, please email: APSIMConference@gov.nl.ca.

We hope to see you there!

Privacy Management Programs

The OIPC Privacy Management Program framework and related training delivered at a recent OIPC Workshop are now available on our website.

If you have any questions or would like to arrange for an education session for your organization contact: commissioner@oipc.nl.ca.

DESIGNATING THE HEAD OF A LOCAL PUBLIC BODY

Section 109 of the *Access to Information and Protection of Privacy Act, 2015* ("*ATIPPA, 2015*") requires local public bodies - educational bodies; healthcare bodies; and local government bodies – to designate a head and communicate the designation to the Minister of Justice and Public Safety. The head of the local public body (the "Head") may be an individual or a group of individuals and those selected may be staff, board member(s) or elected official(s). Once designated the Head is responsible for all actions and decisions of a public body in relation to the *ATIPPA, 2015*.

Considerations When Designating a Group of Individuals as the Head

When considering designating a group of persons to act as the Head, local public bodies should examine the implications of such a choice.

Factors to be considered include:

- what will be considered a quorum amongst the group;
- the need to establish a quorum when making decisions and taking necessary actions under the *ATIPPA, 2015*;
- the possibility that one or more members of the group may be absent at any given time;
- conflicts of interest; and
- the need to meet legislative timeframes.

Considerations When Designating an Individual as the Head

When designating an individual as the Head, except in extremely limited circumstances, the Head and the ATIPP Coordinator should not be the same individual. Allowing the same individual to be both the Head and the ATIPP Coordinator gives rise to concerns surrounding the possibility of the individual focusing on the identity of the requester rather than the merit of the request. Public bodies must also be mindful that, unlike the Head, the *ATIPPA, 2015* requires that the ATIPP Coordinator be on the staff of the public body.

**A full guidance piece on this topic will soon be available on our website. **

PRACTICE TIP

When you receive notification from the OIPC of an Access Complaint, be sure to index your response by numbering the pages in the records you send to us and provide a table of contents. This will assist both you and the assigned Access and Privacy Analyst when referring to the records.

Similarly, providing a highlighted copy of the responsive records where the highlighted portion reflects what information was redacted in the Applicant's copy will facilitate a smoother review process.

THE IMPORTANCE OF AUDITING ACCESS

In circumstances where employees are permitted access to personal information in order to carry out their employment duties, the public body should have the ability to: i) monitor such access and ii) assess or audit whether instances of access are authorized.

In consultation with information management, IT and records management staff, public bodies should develop a policy and procedure for monitoring and assessing access to personal information. These policies and procedures should address such things as:

- who should conduct audits;
- when audits should be conducted; consider both random and planned audits;
- what information is being accessed and, thereby, what areas will need to be audited; and
- what circumstances will require additional investigation. Consider common areas of concern such as accessing personal information of persons with the same last name or address; accessing the information of well-recognized members of the public; and repeated accesses to the same file or information.

It is important to utilize random audits in addition to planned audits, as both are a means of deterring inappropriate access and also identifying additional areas of concern.

An important part of being able to conduct thorough audits is maintaining a detailed listing of all personal information in the custody and control of the public body — a personal information inventory — including the location and format of that information.

RETENTION OF RECORDS

Section 65 of the *ATIPPA, 2015* states:

> *65. (1) Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.*
>
> *(2) A public body that has custody or control of personal information that is the subject of a request for access to a record or correction of personal information under Part II shall retain that information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request*.

Public bodies are reminded that the obligations set out in section 65 are paramount to records retention policies. When an access to information or correction of information request is received by a public body, the records to which the request relates must not be destroyed, regardless of any retention schedule or policy of the public body, until all aspects of the request, inclusive of appeals and court proceedings, have concluded.

The Commissioner has discussed the issue of destroying records after the receipt of an access request in Report A-2007-019 and, more recently, in Report A-2018-005.

BALANCING WORKLOAD AND STATUTORY DEADLINES

Our most recent Annual Report highlighted the increase in the number of access requests received by public bodies. We also acknowledged the challenge faced by public bodies as a result of this "new normal", but stressed the need for public bodies to adapt. We offered two solutions: increasing resources; or making "presumptively accessible" information readily available without the need for an access to information request.

Recent Report A-2018-006 emphasizes the need for public bodies to ensure that they avail of one or both of the solutions above to ensure that both the routine business of a public body and the work surrounding ATIPP requests proceed without delay. The Report also reminds coordinators to avail of the tools provided for in the *ATIPPA, 2015* which are designed to address exceptional situations: time extensions; disregards; and the variation of a time limit.

PRIVACY TRAINING EXPECTATIONS

Section 110 (1)(d) of the *ATIPPA, 2015* requires ATIPP Coordinators to educate staff about the *Act,* including the privacy provisions. Additionally, a public body cannot expect to properly collect, use, disclose and protect the personal information in its custody or control if it does not educate its staff on the obligations and responsibilities set out in the *Act.*

This responsibility for privacy training and education is continuous. Public bodies and coordinators must provide training to incoming employees and continue such training throughout the course of employment as a refresher and to ensure that any new developments are incorporated. Similarly, public bodies cannot simply rely on general external training, but instead must adapt training to the particular circumstances of the public body and provide employees with practical applications and considerations.

Simple directions to protect personal information and not to improperly collect, use, access or disclose personal information are insufficient. Equally, public bodies cannot simply develop and disseminate privacy policies and procedures without training staff on their content and implications. Public bodies must ensure that any privacy policies they create are fully understood and employees have the tools necessary to implement those policies and procedures. For example, it is ineffective to have a policy requiring employees to lock personal information in filing cabinets or drawers if employees do not have access to locked cabinets or drawers.

Effective privacy training must instill a culture of privacy within the public body which encompasses all members of the public body. Buy-in from Executive promotes and highlights the value placed on privacy within a public body and provides resources to ensure that all members of the public body understand and appreciate that value.

There are various education and training tools available to public bodies including training from the OIPC; training from the ATIPP Office of the Department of Justice and Public Safety; online training programs offered by the University of Alberta; online training from the International Association of Privacy Professionals; and guidance from other provincial and territorial Information and Privacy Commissioners.

ATIPPA PRIVACY BREACH STATISTICS Jan. 1 - Mar. 31, 2018

During this reporting period (January 1 — March 31, 2018), the OIPC received 58 privacy breach reports from 22 public bodies under the *ATIPPA, 2015*. This is down from the 59 reports from 20 public bodies received in the previous reporting period.

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	
Arts NL	1
City of St. John's	3
College of the North Atlantic	4
Dept. of Advanced Education, Skills & Labour	3
Dept. of Children, Seniors & Social Development	7
Dept. of Fisheries & Land Resources	1
Dept. of Health & Community Services	1
Human Resource Secretariat	4
Dept. of Justice & Public Safety	2
Dept. of Service NL	10
Dept. of Tourism, Culture, Industry, & Innovation	1
Eastern Health	4
Eastern Regional Service Board	1
Memorial University of Newfoundland	4
NALCOR	1
Newfoundland and Labrador English School District	3
Newfoundland and Labrador Housing Corporation	2
Newfoundland and Labrador Legal Aid Commission	1
Royal Newfoundland Constabulary	2
Town of Portugal Cove-St. Philip's	1
Town of Wabana	1
Workplace NL	1

Summary by Type	
Mail Out	17
Email	15
Other	13
In Person	5
Intentional (i.e. willful breach)	3
Technical Malfunction	2
Courier	1
Fax	1
Telephone	1

The OIPC has issued a Tip Sheet on avoiding inadvertent privacy breaches.