ABOVE BOARD

A quarterly newsletter published by the Office of the Information and Privacy Commissioner

Volume 12, Issue 4 October, 2020

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

Telephone:

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

This Issue:

Newfoundland and Labrador Launches COVID Alert App

On September 3, Newfoundland and Labrador became the second Canadian province to implement the Government of Canada's COVID-19 exposure notification system. The app has now been adopted in 8 provinces to report a diagnosis of COVID-19 (it does not presently function in British Columbia, Alberta, or the Territories).

The Office of the Information and Privacy Commissioner (OIPC) has been following the development of COVID Alert and other contact tracing efforts and was engaged from an early stage on its development. The OIPC is satisfied that COVID Alert was developed in accordance with the privacy principles expressed by this Office and our Federal, Provincial and Territorial counterparts in our May 7, 2020 joint statement. It is based on a protocol that does not involve the collection of personal information by a public body or any third party and data is anonymized. Its development received considerable scrutiny by privacy and cybersecurity experts across Canada and around the world and there is cause for a high degree of confidence in its security and protection of personal privacy.

In COVID Alert, the governments of Canada and Newfoundland and Labrador have delivered a tool for exposure notification that operates without the mass collection of personal information. As the Government of Newfoundland and Labrador moves towards more e-services, COVID Alert establishes a high standard for such technological solutions.

For more information about COVID Alert, please see:

- Government of Canada – COVID Alert App
- News Release – Information and Privacy Commissioner Comments on Provincial COVID Alert (September 3, 2020).

Reminders and Updates

Error on Wall Calendar

Please be aware that there is an error on the 2020 business day calendar issued by the OIPC. December 28 is presently highlighted as a holiday (to account for Boxing Day falling on a Saturday). However, pursuant to section 27(1.1) of the *Interpretation Act*, a holiday is only moved to the following day if it falls on a Sunday. December 28, 2020 therefore is a business day for the purpose of calculating deadlines under *ATIPPA, 2015*. The OIPC apologizes for this error.

New Form for Disregard Requests

Earlier this week, ATIPP Coordinators were notified that the OIPC has introduced a new form to be used when applying under section 21 of *ATIPPA, 2015* for approval from the Commissioner to disregard an access request. While deadlines (within 5 business days of receiving the request) and criteria for determining whether to approve an application remain unchanged, this new form is intended to streamline the process for public bodies and clarify the information required to be submitted. In addition to our previous email, the form can be found on our website:

Application to Disregard an Access to Information Request.

Providing Reasons to Applicants

Where a public body has decided to withhold all or part of a record on account of one or more of the exceptions provided in *ATIPPA, 2015*, it is required, at section 17(1)(c)(i), to provide "the reasons for the refusal and the provision of this *Act* on which the refusal is based" in its final response. Given the structure of the provision, it is clear that an access to information applicant is entitled to something more than just a citation of the exception being applied.

Therefore, when notifying an applicant that records are being withheld in whole or in part, the public body should attempt to explain its rationale. This practice is not only for the benefit of the applicant, but also the public body itself – the OIPC often receives complaints which could have been avoided had the public body provided the applicant with reasons for why an exception was applied.

While a public body would not be expected to provide a level of detail that would risk disclosing the very information that is being withheld from disclosure, it should provide a brief comment such as:

- "Information was redacted under section 40 because it disclosed the home address of an employee";
- "These emails were withheld because they were communications between the Department and our solicitor to obtain a legal opinion about this matter"; or
- "The redacted information details policy advice provided to the Minister and must be withheld to protect the ability of staff to openly discuss policy options. Factual information that was submitted along with this advice has been provided."

These simple explanations could be sufficient to avert a complaint to this Office.

Working from Home

When the Government of Newfoundland and Labrador announced a public health emergency on March 16, 2020, many public bodies closed their offices and, where possible, staff worked from home. Since June 25, the province has been at alert level 2 and many offices have largely returned to something approaching normal operations. However, many public body employees continue to work remotely from home. While working from home offers benefits in terms of reducing employee density in the workplace and accommodating childcare needs, public bodies need to recognize that this also creates the potential for new challenges and risks to information access, information security, and privacy.

Staff should be reminded that the public body's policies and practices regarding privacy, information management, information security and access remain in effect while staff are working from home. Further, the public body's obligations under *ATIPPA, 2015*, including the protection of personal information and fulfilling the public's right of access to public body information continue to apply. Staff working from home must still report any information security incidents and privacy breaches to their supervisor and/or the public body's ATIPP Coordinator. The normal requirements to notify the Commissioner and affected individuals about the breach of course also continue, as do all of the other protocols for responding to a privacy breach.

While work is being conducted from home, the public body must take reasonable measures to ensure records are preserved. Any records produced by staff whether in the office or while working from home are subject to *ATIPPA, 2015*, and public bodies must be prepared to search for and review responsive records wherever they may be located. This includes any records which may reside on a personal email account (see also: Office of the Chief Information Officer Directive on "Use of Non-Government Email Accounts for Work Purposes"). If staff are using personal devices, reasonable measures should be taken to back-up records to protect them from loss.

Public bodies should advise staff to set up a private workspace in their home, and require that staff take all reasonable measures to protect information and privacy. A workspace should provide privacy for telephone conversations and protect computer screens from being viewed by others in the household. Devices and work-related papers should be secured when not in use.

When using telephone or internet conferencing services (such as Zoom, Webex, Microsoft Teams, Skype, or Google Meet), public bodies should establish rules for all parties regarding what type of information may be exchanged in order to protect privacy. Some public bodies have conducted privacy and security reviews of the different virtual meeting platforms and have authorized specific ones for use. Employees must be sure to comply with these directives. Links or teleconference ID information should be protected to ensure calls cannot be accessed by uninvited parties. Software should be updated to the most current version to maximize security. If possible, a wholly web-based version that does not require the installation of software may be preferred as it helps ensure the most recent version is being used.

The OCIO has also released Information Management and Protection Tips for Working Remotely

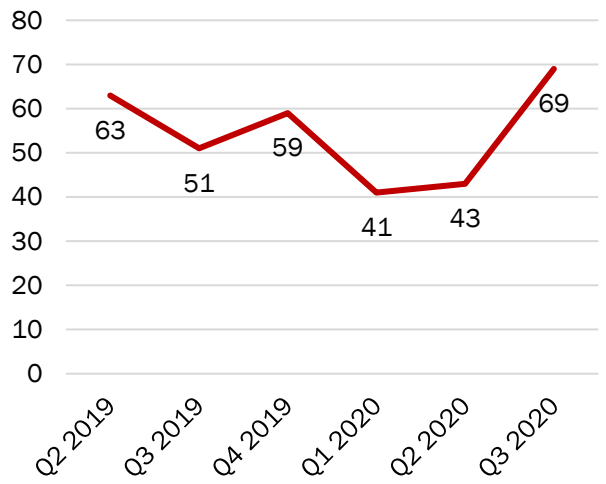
ATIPPA, 2015 Privacy Breach Statistics July 1 to September 30, 2020

During the third quarter of 2020 (July 1 to September 30), the OIPC received 69 privacy breach reports from 27 public bodies under *ATIPPA, 2015*. This is a significant increase from the 43 breaches reported during the previous quarter.

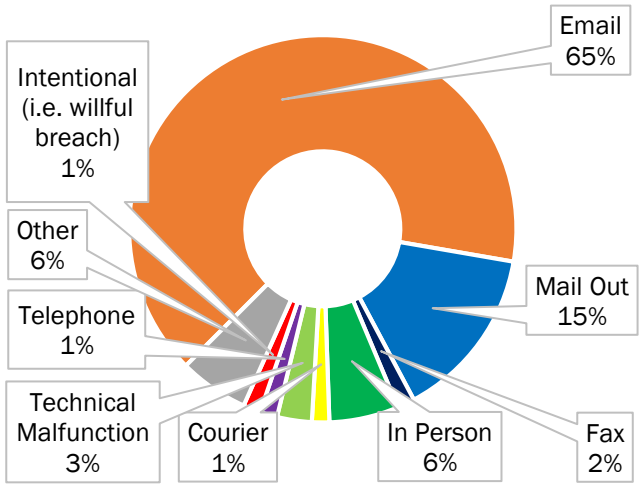
If any public body would like the OIPC to deliver training regarding privacy breaches, or any other topic relating to access or privacy, please contact our Office to arrange a time.

Summary by Public Body	
Central Health	2
City of Corner Brook	1
College of the North Atlantic	10
Department of Advanced Education, Skills and Labour	1
Department of Children, Seniors and Social Development	4
Department of Digital Government and Service NL	10
Department of Education	1
Department of Finance	1
Department of Fisheries and Land Resources	1
Department of Health and Community Services	1
Department of Immigration, Skills and Labour	9
Department of Transportation and Works	1
Eastern Health	1
Human Resource Secretariat	2
Labour Relations Board	1
Memorial University	5
Nalcor Energy	1
Newfoundland and Labrador Housing Corporation	3
Newfoundland and Labrador Legal Aid Commission	6
Office of the Chief Information Officer	1
Office of the Controller General	1
Office of the Public Trustee	1
Public Service Commission	1
Royal Newfoundland Constabulary	1
Town of Channel-Port Aux Basques	1
Western Health	1
Workplace NL	1

Trends



Summary by Type



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