ABOVE BOARD

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

Volume 14, Issue 1 January 2022

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:

- Privacy and the Cyber Attack on the NL Health System
- What is a Cyber Attack?
- Transferring a Request
- New Year Resolutions
- Duty to Discuss: OIPC Podcast
- Section 33 (Workplace Investigation) Guidance Updated
- Training Opportunities
- *ATIPPA, 2015* Privacy Breach Statistics October 1 – December 31, 2021
- New Guidance Alert – Yes You Can!

Privacy and the Cyber Attack on the NL Health System

Anyone who believes their personal information or personal health information may have been accessed or stolen as a result of the cyber attack on our health system has a right to file a complaint with the NL OIPC. We wish to advise, however, that the Information and Privacy Commissioner has already decided to launch a privacy investigation. Unless you believe there are very specific circumstances particular to your own case that would warrant an individual complaint, it won't be necessary for individuals to file a complaint. If you have any questions or aren't sure if you should file an individual complaint, feel free to contact our Office to discuss further.

For more information about the cyber attack and how it has impacted the health system and the personal information of residents, it is recommended that you refer to the resources prepared by the Department of Health and Community Services or use the Department's toll free number (1-833-718-3021).

What is a Cyber Attack?

We have all seen the news of the cyber attack that impacted the health sector. While it is too early to discuss specific details of this particular attack, we wanted to provide general information about such attacks and remind you of the steps the Department has identified to help you protect yourself.

The Canadian Centre for Cyber Security (Cyber Centre) is Canada's authority on cyber security. The Cyber Centre defines a cyber attack as the "use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device."

The Cyber Centre issued a publication titled, National Cyber Threat Assessment 2020, and it contains a few key judgements of particular interest, as they may help readers better understand the threat environment facing entities today:

- *The number of cyber threat actors is rising, and they are becoming more sophisticated. The commercial sale of cyber tools coupled with a global pool of talent has resulted in more threat actors and more sophisticated threat activity. Illegal online markets for cyber tools and services have also allowed cybercriminals to conduct more complex and sophisticated campaigns.*

- *Cybercrime continues to be the cyber threat that is most likely to affect Canadians and Canadian organizations. We assess that, almost certainly, over the next two years, Canadians and Canadian organizations will continue to face online fraud and attempts to steal personal, financial, and corporate information.*

The Department has provided a list of resources of how you can protect your information; see their FAQ page for the cyber attack. The Privacy Commissioner of Canada also has Identity Theft resources and the Government of Canada has tips on cyber safety on its Get Cyber Safe website. While not a Canadian resource, the Australian Cyber Security Centre has great tips on how to protect yourself, as well as some common warning signs that your identity may be compromised. And for anyone looking for more information on staying safe online and securing accounts, the National Cyber Security Alliance has a number of resources that may assist.

Transferring a Request

Section 14 of *ATIPPA, 2015* establishes the ability for a public body to transfer a request within five days of receipt of the request where:

- the record was produced by or for the other public body; or
- the record or personal information is in the custody of or under the control of the other public body.

When transferring a request, the applicant must be notified in writing and the public body to which the request is transferred must respond to the request as if it had originally been made to them, using the date of the transfer as the date the request was received.

Section 3.5 of the ATIPP Office's *Access to Information: Policy and Procedures Manual* outlines the process that should be followed when transferring a request. It states, in part:

> *Where a public body who receives a request knows that another public body has the records sought by the applicant, the request should be transferred rather than advising the applicant that there are no responsive records and closing the request. This is consistent with the duty to assist. Before*

> *transferring an ATIPP request to another public body, the ATIPP Coordinator should make sure that the second public body has the requested records and is the correct public body to which the request should be transferred.*

Coordinators should not transfer a request to a public body that has indicated that it does not have any responsive records or transfer based on an assumption that they may have responsive records. Such actions may be considered contrary to the duty to assist. While transferring a request is discretionary, the duty to assist the applicant is mandatory.

On the surface, it appears that *ATIPPA, 2015* does not contemplate a partial transfer of a request. However, commissioner reports from this and other jurisdictions demonstrate support for this practice where appropriate. If a coordinator determines that part of the request should be transferred, it should be clear in identifying the part of the request that is being processed by them, and what part has been transferred to the other public body. If the public body has some responsive records and is aware that another public body has additional records, as part of the duty to assist, the coordinator could consider making the applicant aware of this fact, as the applicant may wish to make a separate application to that public body (see Report A-2020-007 on this point).

If an ATIPP request is transferred, the public body transferring the request must notify the applicant of the transfer in writing. The transfer process should be done as efficiently and promptly as possible.

Another consideration in the transferring process is section 12, anonymity of the applicant. The limit on disclosure applies until the final response to the request has been sent to the applicant. However, section 12(2)(b) states, "Subsection (1) does not apply to a request …(b) where the name of the applicant is necessary to respond to the request and the applicant has consented to its disclosure." Another consideration is section 68(1)(c), which states, "A public body may disclose personal information only…(c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in section 69." While our Office has not interpreted these sections in relation to transferring a request in a report, it would be good practice for coordinators to consider the applicant's privacy expectations prior to transferring the request and disclosing their name to another public body.

OIPC recognizes that there are legislative timelines to consider and not all applicants respond promptly. However, if a privacy complaint were to be received, we would examine the steps taken to contact the applicant and/or the consideration the public body gave to the applicant's privacy prior to transferring the request.

New Year Resolutions

Many people take time at the beginning of a new year to reflect on the past year and set goals and objectives for the upcoming year. With so many daily demands with legislative deadlines associated with them, sometimes other duties can fall off the radar.

Privacy

For the majority of coordinators, the focus is on the day-to-day demands of access, with little time to focus on compliance with Part III of *ATIPPA, 2015*, the Protection of Personal Information. Our Office has published a number of guidance pieces that can assist with compliance, including resources on Privacy Impact Assessments (PIAs) and Privacy Management Programs (PMPs). If your

entity doesn't have a PMP and/or isn't sure what assessments have been conducted, 2022 is a good year to get on top of these gaps.

If you start work documenting the personal information held by your public body in January, you'll have a personal information inventory completed before you know it! This is a critical first step in any PMP. Further, it is a good idea to proactively identify what, if any privacy assessment was done on the system that holds the information and determine if it needs to be updated.

Coordinators are reminded that, if a breach or privacy complaint were to be received by our Office, we would ask about your entity's PMP; if it involved a specific system or process, we would also ask about any PIA that was conducted. As this guidance has been out for a number of years, we would expect to see progress on compliance, if not full compliance.

Information Management

Information management is an important part of our work lives, however we can fall behind, especially during busy times. Why not set a re-occurring meeting in your calendar each week and take 30-60 minutes to ensure all records from the week are either placed in the appropriate records management system or destroyed (if they are transitory)? Your future self will thank you for being so organized!

Professional Development

When work is busy, it can be difficult to find the time to invest in yourself to stay on top of your profession. While attending conferences can require a financial investment, there are many opportunities available that only cost your time. For members of the International Association of Privacy Professionals (IAPP), there are great web conferences available at no cost. The ATIPP Office offers regular Community of Practice sessions for coordinators. Both the ATIPP Office and ourselves offer training, even customized training, upon request. So be sure to work time into your calendar to stay current and mingle with others in the profession. Your fellow coordinators will no doubt have tips and tricks that will make the access process more efficient or assist you with specific challenges.

Duty to Discuss: OIPC Podcast

Episode 4 of our podcast *Duty to Discuss* has been published! In this episode, Commissioner Harvey chats with Dr. Jonathan Anderson, who is with Memorial University's Faculty of Engineering and Applied Science, about computer security and privacy.

Section 33 (Workplace Investigation) Guidance Updated

In light of two recent decisions from the Supreme Court of Newfoundland and Labrador that have substantially affected how section 33 is to be interpreted in relation to other exceptions under *ATIPPA, 2015*, OIPC has issued updated guidance.

In College of the North Atlantic (R3), 2021 NLSC 120, the Court held that section 33(3) does not override the provisions of section 40. Section 33(3) and section 40(1) cannot be read in isolation; as both are mandatory exceptions, where personal information is concerned, both sections must be read together in context with section 40(5).

In Oleynik v. Memorial University of Newfoundland and Labrador, 2021 NLSC 51, the Court determined that section 33(3) does not override section 30, nor does it abrogate solicitor-client or litigation privilege.

Training Opportunities

Information Management Policies and Procedures

ARMA (Association of Records Managers & Administrators) Terra Nova and Lewis Eisen have partnered to offer an online workshop series *Drafting Effective Information Management Policies.* There will be 3 sessions (2.5 hours each) over three days (January 25-27, 2022) from 12:30 am - 3:00 pm (NDT). Space is limited, so request your seat by registering here: https://www.eventbrite.ca/e/drafting-effective-information-management-policies-tickets-228869523907 . The cost to participate varies and is available online. If you need additional information, please contact ARMA Terra Nova: armaterranovanl@gmail.com.

Municipal ATIPP Coordinators

The ATIPP Office offers training sessions designed specifically for municipal ATIPP coordinators, presently being delivered virtually over Zoom. OIPC encourages all coordinators to attend. The next scheduled sessions are as follows (please note that after January sessions, training will be moving to a four-hour format):

- January 11th and 12th -11:00 am to 12:30 pm each day
- January 25th and 26th -11:00 am to 12:30 pm each day
- March 1st and 2nd -10:30 to 12:30 each day
- March 29th and 30th – 10:30 to 12:30 each day
- April 26th and 27th – 10:30 to 12:30 each day
- May 31st and June 1st – 10:30 to 12:30 each day

Interested individuals should contact Jacob Kimball at JacobKimball@gov.nl.ca no later than the end of business on the Friday prior to the session.

ATIPPA, 2015 Privacy Breach Statistics October 1 – December 31, 2021

During the final quarter of 2021 (October 1- December 31, 2021) the OIPC received 63 privacy breach reports from 25 public bodies under *ATIPPA, 2015*; 35 of the breaches involved email. Public bodies are reminded that tips on avoiding breaches can be found here.

Five intentional breaches were reported; four of these involve the cyber attack on the health system. A statement regarding the cyber attack is on our website. The fifth involved the City of St. Johns, when a workplace investigation report was leaked to the media. While the investigation continues, the City noted that, when the reports were initially provided, all receiving parties were asked to keep the report confidential and respect the privacy of the individuals involved.

New Guidance Alert – OIPC and the Office of the Child and Youth Advocate have issued a new guidance piece, *Yes You Can! Dispelling the Myths About Sharing Information Relating to Children and Youth Who Receive Government Services*.