SAFEGUARD

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

Volume 4, Issue 2 May, 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

In This Issue:

Message from OIPC on COVID-19 Pandemic

The ongoing COVID-19 pandemic has presented health care professionals and custodians of personal health information with significant challenges as they provide health care to the people of Newfoundland and Labrador. The Office of the Information and Privacy Commissioner (OIPC) would like to recognize the efforts of those working in the health care sector during these trying times.

This pandemic presents not only challenges in the provision of health care, but also in meeting custodians' privacy obligations under the *Personal Health Information Act* (*PHIA*). Responses to the pandemic require increased sharing of personal health information between custodians and regional health authorities, and with the Department of Health and Community Services. More personal information and personal health information might be collected at this time, especially in contact tracing efforts to determine who might have come into contact with the virus. Anxiety about the spread of COVID-19 may prompt custodians or staff to improperly seek out information about the health status of patients through their records of health information. In spite of all of this, we are aware that custodians in the Province continue to endeavor to follow *PHIA*, safeguard personal health information and investigate alleged privacy breaches as they arise.

The OIPC is presently working remotely. While we are continuing to receive and respond to access and privacy complaints under *PHIA* and the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*), our Office has been granted an extension by the Supreme Court of Newfoundland and Labrador to some deadlines until we return to normal operations.

During this time, the OIPC has prepared several guidance documents for public bodies and custodians which we will highlight in this issue of Safeguard.

Protecting Privacy and Security while Working from Home

Since March 16, 2020, the Government of Newfoundland and Labrador has implemented its Business Continuity Plan and many public service staff, including the OIPC, are working remotely. Many private sector employees are also working remotely from home, even with the May 11 announcement allowing some low-risk workplaces, such as professional services firms, to re-open.

Working from home presents potential risks and challenges for protecting privacy as well as the security of any information – especially personal information or personal health information – transmitted over an internet connection or conveyed through video conferencing software. Popular platforms for business conferencing being utilized today include Zoom (Zoom Video Communications, Inc.), Webex (Cisco Systems Inc.), Skype and Teams (Microsoft), Slack (Slack Technologies), FaceTime (Apple) and Google Meet, Google Duo, and Google Hangouts.

The Canadian Centre for Cyber Security has issued several alerts, as well as guidance, surrounding the use of these services and protecting privacy and security while working from home. The Canadian Centre for Cyber Security is a division of the Government of Canada's Communications Security Establishment responsible for providing guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public. Particularly relevant recent alerts include:

- March 20, 2020: Cyber threats to Canadian health organizations (AL20-008)
- April 14, 2020: Considerations when using video-teleconference products and services (AL20-011)
- May 2020: Security Tips for Organizations with Remote Workers (ITSAP.10.016)

In addition to the guidance provided by the Canadian Centre for Cyber Security and the Communications Security Establishment, custodians of health information and public bodies are advised to adhere to the following general guidelines when using online services.

- Ensure the software you are using has been updated to the current version. 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.
- Establish rules for all parties regarding what type of information may be exchanged. For example, a custodian may decide that the names of patients or other personal health information will not be discussed but will instead be exchanged through other methods such as secure email.
- Protect links or teleconference ID information to ensure conferences cannot be accessed by uninvited parties.

All public bodies and custodians should review and ensure they understand the terms and privacy policies for any software or platform prior to use. It is your responsibility to ensure that the software you are using allows you to fulfill your obligations under *PHIA* and *ATIPPA, 2015*.

Framework to Assess Privacy-Impactful Initiatives in Response to COVID-19

The safety and security of the public is of grave concern in the current COVID-19 health crisis. The urgency of limiting the spread of the virus is understandably a significant challenge for government and public health authorities, who are looking for ways to leverage personal information and "Big Data" to contain and gain insights about the novel virus and the global threat it presents. In this context, we may see more extraordinary measures being contemplated. Some of these new measures may not be voluntary, and perhaps certain measures that are currently voluntary will become mandatory. Some of these measures will have significant implications for privacy and civil liberties.

During a public health crisis, privacy laws and other protections still apply, but they are not a barrier to the appropriate collection, use and sharing of information. When reasonably and contextually interpreted, existing privacy legislation, norms and best practices for data collection, use and disclosure ensure responsible data use while also allowing sharing that supports public health. They also promote continued trust in our health system and in government generally.

All public bodies and custodians must continue to operate under lawful authority and act responsibly, particularly with respect to handling personal health information, and information about individuals' travel, movements and contacts or association all of which are generally considered sensitive.

Privacy protection is not just a set of technical rules and regulations, but rather represents a continuing imperative to preserve fundamental human rights and democratic values, even in exceptional circumstances. Public bodies and custodians should still apply the principles of necessity and proportionality, whether in applying existing measures or in deciding on new actions to address the current crisis. Purpose limitation, that is, ensuring that personal information collected, used or disclosed for public health reasons is not used for other reasons, is particularly important in current circumstances. How personal information is safeguarded, and how long it is retained after the crisis, is also crucial.

The COVID-19 public health crisis has raised exceptionally difficult challenges to both privacy and public health. The OIPC has prepared a list of key privacy principles that should factor into any assessment of measures proposed to combat COVID-19 that have an impact on the privacy of residents of the Province of Newfoundland and Labrador. Our Office's "A Framework for the Government of Newfoundland and Labrador to Assess Privacy-Impactful Initiatives in Response to COVID-19" can be accessed here.

This Guidance is based on a similar piece published by the Office of the Privacy Commissioner of Canada, whose permission to adapt this for the Province of Newfoundland and Labrador context is gratefully acknowledged.

For further information regarding private industry and federal government departments which are outside the jurisdiction of the OIPC, the Office of the Privacy Commissioner of Canada has issued guidance to help organizations subject to federal privacy laws understand their privacy-related obligations during the COVID-19 outbreak. For guidance on other privacy principles that continue to apply, please read: "Expectations: OPC's Guide to the Privacy Impact Assessment Process".

What to Do and How to Communicate in an Emergency

Emergencies do not supplant the need for privacy but they do impact it. While privacy should still be protected where possible, the need for complete and accurate information flow in a crisis is critical. Do not let privacy considerations put anyone's health at risk.

PHIA, as well as *ATIPPA, 2015*, have been designed to accommodate these circumstances. The OIPC has developed a slide deck, "Don't Blame Privacy – What to Do and How to Communicate in an Emergency" to inform public bodies and custodians about information collection, use and disclosure in emergency situations.

If you have questions, please contact our Office.

Don't Blame Privacy – What to Do and How to Communicate in an Emergency

Canadian Privacy Commissioners Issue Joint Statement on Contact Tracing Apps

On May 7, the Newfoundland and Labrador Office of the Information and Privacy Commissioner joined Canada's Federal, Provincial and Territorial Privacy Commissioners in issuing a joint statement regarding the development of smartphone-based digital contact tracing apps.

These apps are being explored in Newfoundland and Labrador and many other jurisdictions in Canada and around the world. They are new tools that, if effective, might add to the current public health initiatives required to respond to the ongoing COVID-19 pandemic.

Commissioners agreed that "Some of these measures will have significant implications for privacy and other fundamental rights. The choices that our governments make today about how to achieve both public health protection and respect for our fundamental Canadian values, including the right to privacy, will shape the future of our country."

The resolution includes a series of principles, arising from Canada's privacy statutes and relevant best practices that governments, health agencies, and commercial third parties are encouraged to follow in the development and implementation of these applications.

The position of this Office is that such initiatives, if properly implemented, and if proven effective, may leverage today's modern technology to simultaneously achieve both greater public health protection and the protection of privacy as a fundamental human right. However, improperly implemented, tracing apps could involve the state or corporate surveillance of Canadians beyond that justified by the public health need and risk the misuse of our personal information.

You can access our Office's news release and the joint statement here.

APSIM 2020

Originally scheduled for the last week of April, APSIM has been postponed on account of the ongoing COVID-19 pandemic. The OIPC will provide an update on a new date as soon as possible.