SAFEGUARD

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

Volume 5, Issue 1 February 2021

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:

APSIM Conference

Newfoundland and Labrador's semi-annual Access, Privacy, Security and Information Management (APSIM) Conference will be taking place this year from March 16 to March 18. In keeping with social distancing guidelines, the conference will be held online. Keynote speakers include former British Columbia Information and Privacy Commissioner David Loukidelis and University of Ottawa law professor Dr. Teresa Scassa. Everyone is invited to attend!

More information can be found on the APSIM website in the coming days.

Registration is available at Register - APSIM Conference 2018 (gov.nl.ca).

Main Takeaways from Canada's COVID Healthcare Innovation

As has been demonstrated by the quick adaptation of many in the health sector to the evolving nature of COVID-19, Canada has been at the forefront of developing new and innovative technologies and techniques to address the health needs of Canadians.

A recent article published by Microsoft outlined some views about the impact of health innovation in 2020 and where that might lead Canada in the future. At the OIPC, we see these and other impacts, some of which will require close attention from privacy regulators to ensure that privacy is an integral part of these new innovations. The impacts identified by the article include the following:

1. Virtual healthcare will be a permanent aspect of healthcare.

   Although the number of in-person visits has diminished due to safety protocols, virtual physician visits have increased drastically. These virtual visits are beneficial to individuals with mobility issues, those who are immunocompromised, and individuals living in rural areas or areas without regular access to healthcare providers.

   Physicians and patients alike have taken advantage of pre-existing software to make these appointments possible and to connect.

   At Ontario's Lakeridge Health, the primary health care provider saw an 800 percent increase in virtual services, creating over 30 new clinics within the first few weeks of the pandemic.

   Although the widespread adaptation of virtual healthcare was born out of necessity, the benefits of offering virtual healthcare to all individuals has been demonstrated. It seems these options, fixing issues relating to accessibility and convenience, are here to stay.

2. It is crucial to continue to balance innovation with privacy, security, and compliance.

   As more healthcare services continue to operate online and in a digital sphere, it is critical to remain vigilant about privacy and security risks. According to the Canadian Centre for Cyber Security, Canada's healthcare system is facing increasing threats from bad actors trying to access personal health information, and the COVID-19 pandemic has exacerbated the situation.

   As the healthcare sector continues to create and innovate, privacy, security, and compliance with privacy legislation must remain at the forefront. Developers must build privacy into the front-end of their systems instead of making it an afterthought.

3. Innovation will continue to shape healthcare in Canada.

   Provinces, physicians, and other healthcare providers are working with business and other stakeholders to leverage digital tools to enhance patient experiences. Recent examples listed in Microsoft's article include the development of Artificial Intelligence (AI) to monitor the effectiveness of social distancing polices at a Vancouver hospital and the use of AI by biomedical researchers in cancer treatments.

In the local context, the NL Centre for Health Innovation (NLCHI) at its Annual General Meeting in September 2020 also noted that they have been quick to build on and implement new technologies for virtual care and predictive analytics. They also note that the pandemic has allowed thousands of healthcare employees to work remotely from home.

Stephen Clark, CEO of NLCHI noted,

> *The digital aspect of health care is advancing quickly and NLCHI is at the forefront. Over the past year we have expanded and enhanced technology solutions to deliver quality health information, supported system and process improvements and identified and delivered dynamic and innovative solutions to enable the province to achieve improved health outcomes. Much of this work was fast-tracked due to COVID-19 and I am very proud of the team's efforts to support the provincial response to the pandemic.*

It is clear that innovation-drivers throughout the health technology space are now taking stock of how far we have come in the past year, from the biggest international players to the local level. As we move through the vaccine roll-out and towards (hopefully) a return to "normal", the OIPC will continue to monitor changes and trends so that as these innovations come along we can work with health information custodians to help ensure that privacy protections remain an integral part of what they do.

Saskatchewan eHealth Ransomware Reports

In December 2020, Saskatchewan's Auditor General released a Report (Volume 2) that critically examined IT network access and the testing of disaster recovery plans at eHealth Saskatchewan (eHealth). On a similar topic, OIPC Saskatchewan released Investigation Report 009-2020, 053-2020, 224-2020. Both Reports were prompted by a ransomware attack in 2019/2020 that impacted various health entities in that province. Both provide considerations and lessons for custodians in this province.

In late December 2019, a computer with access to eHealth's IT network was the target of a spear phishing attack. This attack remained undetected by eHealth until it led to a larger ransomware attack in early January 2020. Containment efforts required restoring data using back-up systems, which resulted in the unavailability of a number of essential systems, some for an extended period.

From the Auditor General's Report

In 2017, eHealth Saskatchewan was directed to consolidate IT services provided by a number of major trustees into a single service. The Report notes that "eHealth does not have a single set of IT policies or processes and staff within the Authority to continue to provide IT services."

Although Service Level Agreements (SLAs) establish common understandings on important matters like the services that must be provided, security and disaster recovery requirements, and more, an updated SLA had not been signed. eHealth did not have disaster recovery plans and had not conducted testing of plans for critical systems. As of March 31, 2020, eHealth had completed a recovery playbook for seven of the 38 critical systems.

The Auditor General also noted

> *"eHealth did not sufficiently control access to the eHealth IT network, evaluate the effectiveness of its network access controls, or effectively monitor network security logs to detect or prevent malicious activity on the eHealth IT network in 2019-20. […] Controlling IT network access helps mitigate the risk of security breaches, and the extent of breaches. Effective IT network monitoring helps timely detection of malicious activity and mitigate the risks of a successful attack on its corporate network."*

Saskatchewan OIPC Report

In this Commissioner's Report, it was concluded that the ransomware incident was a breach involving the most sensitive information of residents. The Commissioner made a significant number of recommendations regarding preventative and mitigating cybersecurity measures for eHealth going forward.

Many recommendations refer to a SaskTel Report. During OIPC's investigation, it learned through the Ministry of Health that eHealth had an 870 page technical report prepared by Saskatchewan Telecommunications (SaskTel) dated May 4, 2020. eHealth engaged SaskTel to assist in incident response, including a security architect, digital forensics (two employees) and corporate security, which resulted in an 840 page Digital Forensic Analysis (SaskTel Report/DFA) report. Recommendations in the final OIPC Report that reference this report include ones regarding cyber security maturity, incident response, and others.

OIPC Podcast - Duty to Discuss

As part of its mandate to advocate on access and privacy matters, the OIPC recently created a podcast entitled "Duty to Discuss". The release of the podcast also coincided with the internationally-celebrated Data Privacy Day.

In the inaugural episode, Commissioner Michael Harvey chats with Dr. Chandra Kavanagh of Bounce Health Innovation about the types of health-based technology being developed in Newfoundland and Labrador. The pair also discuss Bounce's regulatory compliance package which assists entrepreneurs build privacy into their products at the outset of development, instead of making privacy an afterthought.

To listen to Duty to Discuss, please visit our podcast page or search for the podcast on Google, Apple, or Spotify.

Commissioner Michael Harvey (left) and Dr. Chandra Kavanagh (right) during the recording of the Duty to Discuss inaugural episode in celebration of Data Privacy Day on January 28, 2021.

Complaints and Breach Notifications

Between December 1, 2020 and February 25, 2021, the OIPC received the following breach notifications and complaints related to *PHIA.*

- Ten breach notifications were sent to this Office following an incident. The majority of these breaches occurred within the regional health authorities.

- The OIPC received three complaints related to PHIA during the same period of time.

Per section 15(4) of *PHIA*, material breaches – inappropriate collection, use, or disclosure of personal health information – must be reported to the Commissioner via the breach reporting form from the OIPC.