



SAFEGUARD

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

Volume 8, Issue 4

November 2024

Contact Information

Office of the Information and Privacy Commissioner

Mailing Address:
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

Website:

www.oipc.nl.ca

Follow us on social media!

LinkedIn:

<https://www.linkedin.com/company/oipc-nl>

This Issue:

- APSIM Conference November 28-29, 2024
- Joint Investigation into LifeLabs Data Breach Released
- Recent Presentation to Small Custodians
- Right to Know Week 2024 - Recap
- PHIA Privacy Breach Statistics August 1, 2024 - October 31, 2024

APSIM Conference November 28-29, 2024

The Access, Privacy, Security and Information Management (APSIM) Conference took place on November 28 and 29, 2024 and it was a great success!



This was our first in-person conference in several years, and it was held at the Health Innovation Acceleration Centre (HIAC) located in St. John's, NL. The conference was aimed at individuals working in the public sector, health care community, and those interested in access, privacy, security, and information management topics.

Keynotes

Our keynote speakers shared their thoughts on AI, cyber security, privacy and the Constitution and the privacy landscape.

The Conference kicked off with our first keynote speaker, Katrina Ingram, who took us on a deep dive into the world of AI and explored the question: is it possible to advance responsible AI? AI is here and used in so many aspects of our lives already. Katrina encouraged attendees to think about how data impacts AI and vice versa, as well as who is using AI and why. She also spoke to future considerations as the world struggles to regulate AI and left attendees to contemplate how to build a responsible AI culture.

Katrina's session was followed by a speaker from our province's own Cyber Security Office as well as two speakers from the Canadian Centre for Cyber Security (CCCS) who took attendees on a journey across the cyber threat landscape. This presentation gave attendees insight into the extent of cyber

activity happening behind the scenes and highlighted that, at times, it is possible to detect these threats in advance and warn organizations. The CCCS presenters even left us with an early Christmas present - a wonderful resource titled [Cyber Security Readiness Goals: Securing our Most Critical Systems!](#)

On the second day of the conference our first keynote speaker presented on privacy as it relates to the Constitution, and the view that it is already a protected right. Kate Robertson raised some interesting thoughts on privacy and how many focus on provincial legislation and forget to consider that privacy is a right protected under the Charter and in the Constitution.

Deputy Federal Privacy Commissioner Marc Chénier followed Kate with a wonderful overview of the privacy landscape and the work that the Office of the Privacy Commissioner of Canada is doing with investigation, guidance, court decisions as well as some of the challenges they face.

Other plenary sessions included a very informative presentation on data governance and why it is important, as well as a lively panel discussion on the role of journalism in access to information and keeping public bodies accountable and transparent featuring some of our local journalists!

Breakout Sessions

We had a total of 11 breakout sessions, each mostly focusing on a particular area of either access to information, privacy, information management, or security, including the following:

- We had two great breakout sessions involving panel discussions. One of the panels discussed **Handling Difficult Conversations**. Panelists in that session shared their thoughts and opinions drawing on their vast experience in access to information and privacy! The panel had great representation from the health, municipal, and government sectors.
- The other panel discussion was focused on **Information Management (IM)**. This panel of experienced professionals shared their insights and strategies to empower attendees to champion IM within their organization with lots of tips and suggestions on how to navigate the difficult challenges facing the IM community.
- Some of the individual sessions included Bill Peddle's presentation on **Large Scale Records Digitization** which was jam packed and highlighted the details and considerations required to make a digitization initiative successful.
- The **Change Management** session, presented by Ronnie Walsh, was energetic and engaging! She really encouraged attendees to consider how change affects individuals in an organization. This presentation highlighted steps that organizations can take to help when transitions are happening and emphasized how communicating with employees and staff helps tremendously in times of change.
- Joe Hines' presentation on **Cybersecurity** was a reminder that all organizations are vulnerable to cyberthreats and highlighted how cyber insurance plays an important role. Attendees were given a rundown of critical and important cyber hygiene requirements organizations need to have!
- Dr. Chandra Kavanagh spoke to attendees about mental health and maintaining psychological health in diverse work environments. An important topic and a great presentation as this affects everyone!

These are just a few highlights from the breakout sessions. To see the full Agenda, the speakers that presented and their materials please visit our [APSIM Conference website](#).

Municipal Workshop

In addition to the in-person APSIM Conference, we also hosted a virtual half-day Municipal Workshop, which took place a few days prior to the conference on November 26, 2024. With the large geographic distribution of municipalities in our province, we wanted to offer something specific to municipalities that they did not need to travel to attend.



This Workshop covered three topics, Information Management, Cybersecurity, and Privacy (CCTV).

IM Session

Our first speaker was Melissa Thorne, Town Clerk and ATIPP Coordinator at the Town of Hughes Brook. She provided great tips for developing policies and procedures for municipalities, using examples from her own experience working in a municipality in Ontario as well as Hughes Brook. She emphasized that policies and procedures are important to guide municipalities (staff and councillors) as they provide a roadmap of how things are supposed to function and keep the municipality accountable to its citizens. Furthermore, policies and procedures play a key role in succession planning. When people leave jobs and when roles change, there needs to be a documented plan so that the functioning of the municipality can continue with as little disruption as possible. Finally, policies and procedures help municipalities figure out what they have – if you don't know where your records are or what kinds of records you have how are you supposed to access them and rely on them when necessary?

Cybersecurity Session

Our second speaker, Brad Hynes from the Town of St. Marys (Ontario) gave us a great behind the scenes look at a cyber incident that happened shortly after he had taken his job with the Town of St. Marys. Brad spoke about how cyber attacks can happen to small, medium, and large municipalities and that it's not about "IF" it will happen, it's about "WHEN" it will happen. He provided insight into the timelines and how fast things went from a normal day to dealing with a cyber attack and how the Town managed this attack. The Town decided to make the public aware of the attack and what was happening and even though in the end the Town ended up paying a ransom to get the information back, the Town learned some valuable lessons and will be entirely more prepared if something like this were to happen again.

Privacy and CCTV Session

Our last speakers were Rod Hynes, Chief Administrative Officer/Clerk of the Town of Pouch Cove, and Erin Drover, Manager at the ATIPP Office, who spoke on Privacy and CCTV. They explained that municipalities should not just be putting up CCTV and surveillance on a whim. There has to be a reason for the surveillance and then the municipality needs to consider the privacy implications. How much information is being captured, how long is it going to be retained, and who has access to that information? These are some of the questions municipalities should be asking before they decide to set up CCTV. As well, towns should have policies and procedures in

place for CCTV before it is used. Rod provided tips from his extensive experience in working with the OIPC on the CCTV Guidelines, his time at the ATIPP Office and his role now as CAO at the Town of Pouch Cove. Municipalities should contact Erin at the ATIPP Office with questions on CCTV as she can provide assistance on the privacy protections that should be in place if the municipality is planning on using CCTV.

We hope that everyone who attended the in-person APSIM Conference here in St. John's enjoyed it and left with information they can take back to their organizations to help in any of the areas of access to information, privacy, information management and security. Similarly, for those who attended the virtual Municipal Workshop, we hope that attendees got some tips to help your municipality.

We wish to thank everyone who helped make the APSIM Conference a success!

Joint Investigation into LifeLabs Data Breach Released

The Office of the Information and Privacy Commissioner of Ontario (ON IPC), together with the Office of the Information and Privacy Commissioner for British Columbia (BC OIPC), published their 2020 [Joint Investigation Report](#) into the 2019 LifeLabs cyber attack.

The Report explains the history of the data breach and the investigation process of the ON IPC and BC OIPC. The Report also offers critical lessons for the entire health care sector to strengthen cyber resilience and privacy protections.

There was a lengthy delay in publishing the Report as LifeLabs had attempted to block the release of the Report through litigation. The Ontario Court of Appeal dismissed LifeLabs' motion for leave to appeal the [Ontario Divisional Court's decision](#), which found that the information in the Report was not privileged or confidential. This is a significant decision for privacy regulators across Canada when assessing organizations' privilege claims over breach investigation reports.

The Breach

On November 1 and 5, 2019, respectively, LifeLabs notified the ON IPC and the BC OIPC of a potential privacy breach under Ontario's **Personal Health Information Protection Act** (PHIPA) and British Columbia's **Personal Information Protection Act** (PIPA). LifeLabs is Canada's largest provider of general health diagnostic and specialty laboratory testing services.

LifeLabs advised that on October 28, 2019, through a security assessment conducted by a third party, it had detected a cyber attack on its computer systems. After locking down the affected systems, LifeLabs was contacted by the attackers. The attackers claimed to have stolen the personal information and personal health information of LifeLabs' customers and threatened to release the information publicly unless LifeLabs paid a ransom. The attackers provided LifeLabs with a sample of the personal information and personal health information they had stolen.

After additional correspondence to substantiate the attackers' claims, LifeLabs paid the ransom. The attackers provided LifeLabs with a copy of their report and a substantial amount of data, consisting of the personal information and personal health information of approximately 8.6 million LifeLabs customers, located primarily in Ontario and British Columbia.

The Findings

The ON IPC and BC OIPC made the following findings.

1. LifeLabs failed to take reasonable steps to protect personal information and personal health information in its custody and control from theft, loss, and unauthorized access, collection, use, disclosure, copying, modification, or disposal.
2. LifeLabs failed to have in place and follow policies and information practices that comply with PIPA and PHIPA.
3. LifeLabs collected more personal information and personal health information than is reasonably necessary to meet the purpose for which it was collected.

The ON IPC made the following additional findings.

1. LifeLabs has not implemented a process to notify all individuals about the details of what of their personal health information was compromised without requiring those individuals to make a formal access request. Therefore, LifeLabs has not complied with its obligation to notify affected individuals of the breach at the first reasonable opportunity.
2. LifeLabs' contractual arrangements to provide laboratory services to a hospital is inadequate in defining the parties' respective roles and responsibilities under PHIPA.

The Orders

Below are some of the Orders made to LifeLabs. To read the full list of Orders, please visit the ON IPC website.

- Ensuring that staff are aware of their responsibilities to effectively monitor security alerts.
- Putting in place comprehensive written information practices and policies that are in force and that set out the safeguards that LifeLabs has implemented with respect to information technology security in order to comply with PHIPA and PIPA.
- Ceasing to collect failed login and password pairs and to securely dispose of the records of that information that it has collected.
- Recommending that LifeLabs consult with independent third-party experts with respect to whether a longer period of credit monitoring service would be more appropriate in the circumstances of this breach.

To read the full Report please visit the [ON IPC website](#).

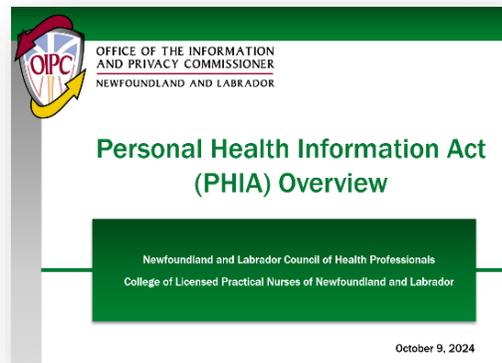
Recent Presentation to Small Custodians

As part of our Office's outreach initiatives, we provide guidance and training on the **Personal Health Information Act** (PHIA). Should custodians be interested in a general presentation on PHIA or wish to focus on specific areas of interest or concern, please contact our Office to discuss scheduling an education session.

Our Office recently presented to the Newfoundland and Labrador Council of Health Professionals (NLCHP) and the College of Licensed Practical Nurses of Newfoundland and Labrador (CLPNNL).

NLCHP oversees a number of different health professionals, including, speech language pathologists/audiologists, respiratory therapists, medical laboratory technologists, midwives and acupuncturists, while the CLPNNL is the regulatory/licensing body for licensed practical nurses (LPNs). Many of these professionals are self-employed and therefore would be considered the custodian responsible for the personal information they hold.

We had great attendance at this session with approximately 100 attendees! We provided a presentation that covered PHIA generally, including a review of who is considered a custodian under PHIA as well as a review of the definition of personal health information. We also reminded custodians that they cannot contract out of PHIA and that ultimately custodians are responsible for the personal health information of their clients and patients until another custodian takes over that responsibility.



NLCHP and CLPNNL flagged some specific areas of interest, including record retention schedules, sharing personal health information with insurance companies, disclosure of personal health information, personal health information of deceased individuals and dealing with personal health information when closing a practice.

We discussed hypothetical scenarios involving some of the areas flagged above and provided as many considerations as possible. Some questions will have a specific answer found in PHIA however, in many instances applying PHIA to the collection, use and disclosure of personal health information is fact dependent. We encourage custodians to contact our Office if they wish to discuss a specific issue in their practice and we will provide a much guidance as we can.

On our website custodians can find resources under our [Custodian Resources webpage](#). The [PHIA Compliance Checklist](#) and the [PHIA Toolkit for Small Custodians](#) provide a good overview of custodians' responsibilities under PHIA.

The Department of Health and Community Services also has a number of resources for custodians, including a PHIA Risk Management Toolkit and a PHIA Online Education Program plus others, all of which can be found on their website <https://www.gov.nl.ca/hcs/phia/>.

Right to Know Week 2024 - Recap

Right to Know Week 2024 (September 23-29, 2024)

Right to Know Day is on September 28th every year. It is an internationally recognized day dedicated to creating awareness about the importance of people's right to access government information, while promoting freedom of information as essential to both democracy and good governance.

Right to Know Day now extends to a week of celebrations, known as Right to Know Week, which took place from September 23-29, 2024.

In celebration of this year's Right to Know Week, three of the Atlantic offices of Information and Privacy Commissioners and the Centre for Law and Democracy came together for a live virtual panel discussion on September 25th and invited everyone to attend.

Nova Scotia's Commissioner, Tricia Ralph, Prince Edward Island's Deputy Commissioner, Maria MacDonald, Newfoundland and Labrador's Director of Research and Quality Assurance, Sean Murray, and Centre for Law and Democracy's Legal Officer, Raphael Vagliano, engaged in a live virtual panel discussion that explored why access rights are foundational to democratic governance and discussed some of the current and pressing challenges to the right of access to information.

We are happy to report that the event was a success! Attendees included a mix of people from all over Canada, from the general public, to professionals, including representatives from government, public bodies, private businesses, and regulatory bodies.

Our Office is happy to have hosted and participated in this virtual event!

During Right to Know Week our Office also:

- issued two news releases: a [general Right to Know Week News Release](#) and another Right to Know Week [News Release promoting the Atlantic Panel Discussion Event](#);
- spoke about Right to Know Week on VOXM's Radio Morning Show; and
- released guidance to assist the general public, in both English and French, titled [How to Make an Access Request/Comment présenter une demande d'accès](#).



PHIA Privacy Breach Statistics August 1, 2024 – October 31, 2024

Between August 1, 2024, and October 31, 2024, PHIA breach notifications decreased with OIPC only receiving five breach notifications. The five breach reports came from five different custodians. Some of the breaches involved personal health information being sent to the wrong individual and one of the breaches involved missing records.

Want Training?

We would like to remind custodians that OIPC offers PHIA training that can be customized to their needs!

Interested custodians should email OIPC at commissioner@oipc.nl.ca.

There are also a number of PHIA resources available on OIPC's [website](#).