SAFEGUARD

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

Volume 10, Issue 1 February 2026

Contact Information

Office of the Information and Privacy Commissioner

Mailing Address:
PO Box 13004, Station A
St. John's, NL A1B 3V8

Telephone:

709-729-6309

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://Linkedin.com/company/oipc-nl

This Issue:

Save the Date! APSIM Conference Returns!

OIPC is delighted to announce the return of the APSIM Conference, scheduled for November 26 and 27, 2026. This two-day in-person event will again take place at the Health Innovation Acceleration Centre in St. John's, and will bring together access, privacy, security, and information management professionals.

Want to be part of this year's APSIM Conference? Submit your speaker proposal for a chance to share your expertise, inspire peers, and shape the conversation on access, privacy, security, and information management.

For the latest updates and information about APSIM, please visit the Conference's official website. If you have questions, please contact APSIMconference@gov.nl.ca.

Updates and Reminders

Reminder: Our Office has updated its breach reporting form and related guidelines. Custodians must use OIPC's updated breach reporting form. Breach reports submitted using any other forms, including forms developed by individual custodians, will be rejected and must be re-submitted on the correct form.

Reminder: We have moved! Ensure your breach notification letters to impacted individuals reflect our new physical address: 5th Floor, Beothuck Building, 20 Crosbie Place, St. John's NL. Our mailing address remains the same: PO Box 13004, Station A, St. John's, NL, A1B 3V8.

OIPC has published its 2024-25 Annual Report. The document includes highlights and activities from the 12-month reporting period, updates on OIPC's report on performance, discussions of investigations, statistics from the year, and more.

If you have any questions or feedback about our forms, guidelines or guidance, including suggestions on topics for guidance resources, please let us know!

OIPC Survey on Guidance, Newsletter and Conference

Thank you to everyone who took the time to respond to our survey! While we continue to analyze the responses and prioritize action, we hope to create a new column in this newsletter that presents a scenario and identifies PHIA considerations. If you have any suggestions for scenarios, please submit them to commissioner@oipc.nl.ca using the subject line "PHIA Scenarios". We are also examining suggestions for new PHIA guidance and training.

Data Privacy Day

January 28 was Data Privacy Day, an internationally recognized day dedicated to creating awareness about the importance of privacy and the protection of personal information. It began on January 28, 2007, to mark the anniversary of Convention 108, the first legally binding international treaty dealing with privacy and data protection.

Privacy has been recognized by the Supreme Court of Canada as a right of all Canadians under the Charter of Rights and Freedoms. In this province, privacy has been protected by law through the **Access to Information and Protection of Privacy Act, 2015** and the **Personal Health Information Act** (PHIA).

Staff at OIPC celebrated by watching IPC Ontario's Privacy Day Event: Trustworthy AI in Health: The Promise, Perils, and Protections, which is available to view online. To learn more about how OIPC marked the day, see our news release.

Snooping: Detecting and Containing Snooping Incidents

In this final article in our series on snooping, we examine the expectations with regard to detecting and containing snooping incidents.

Privacy legislation, including PHIA, require that custodians protect the information in its custody or control. A common safeguard is an auditing program; such programs should establish frequency of audits (for example, each person on staff will be audited once every X months), as well as specific procedures for the investigative process. Many entities enhance auditing activities in response to specific events. For example, health care facilities taking patients in response to high profile events will generally audit all access to the involved-patient's medical records.

One such example is described in the NS OIPC's Investigation Report IR23-01. This Report details breaches that occurred in the weeks following Nova Scotia's tragic mass casualty event on April

18-19, 2020 (April 2020 tragedy). Nova Scotia Health (NSH) proactively monitored employees who were accessing the electronic health records of individuals associated with the events to ensure they had a valid reason to be viewing those records. Once suspicious access was flagged, NSH follow-up occurred to determine if the access was legitimate. The report notes at paragraph 123:

> The NSH Privacy Breach Protocol suggests obtaining notarized affidavits that explain the purpose, use and disclosure of accessed information from employees found to have abused their access. Affidavits are a straightforward tool for minimizing the residual risk that the employee shared information because it requires the employee to swear an oath in front of a commissioner of oaths which has consequences if the employee is not truthful. The report noted that there were inconsistent investigations and follow-up.

The report also highlights the importance of conducting additional audits when suspicious access is found. The report states at paragraph 77:

> Conducting additional audits for a one-year period prior to a confirmed privacy breach is a safeguard specifically designed to identify other potential unauthorized accesses and has been effective in confronting employees who initially lied. Conducting further audits of employee access is a reasonable information practice in these circumstances.

The report also noted gaps and discrepancies between when employees were placed on administrative leave, when their access to electronic systems was suspended and when their employment was terminated or discipline was decided. For example, Employee A was placed on administrative leave on April 21, 2020, until employment was terminated on May 20, 2020; access was not suspended during the administrative leave. Employee C was issued discipline in the form of a one-day suspension; Employee C's access to electronic health records was reinstated after the conclusion of the investigation. Employee F was placed on administrative leave pending the investigation on June 10, 2020 and was terminated on June 19, 2020; access was not terminated until July 6, 2020.

Further, seven of the eight employees under investigation had remote access to applications; without removing access, they remained able to access systems during their leave and throughout the investigation. The report states at paragraph 85:

> When asked about remote access by the employees, the representative of NSH's Human Resources Office thought that placing an employee on administrative leave was essentially the same thing as suspending access to the electronic information systems and had not considered the possibility of remote access by these employees.

The above recognizes how important it is to ensure that all involved individuals understand their roles in an investigation and the benefits of collaboration and communication. These are also discussed in OIPC PEI's Breach Report HI-18-005. This report details suspicious access identified during a regular audit process and emphasizes that custodians with electronic systems should have an audit program that is reasonable in their situations. It notes that, while audits are generally run by Information Technology or Security staff, the report should be interpreted by

someone with more intimate knowledge of the staff member, such as their direct manager, who would know which patients the user was caring for and treating.

The report also emphasizes a change in role that should have triggered a change in access to systems. The province amended the educational qualifications for individuals working as Licensed Practical Nurses (LPNs) effective April 1, 2014. The LPN at the center of the report did not obtain the educational requirements and continued to work as a Personal Care Worker (PCW). While both roles have access to electronic systems, the scope of information they can access is more limited. The report states at paragraph 47:

> In the circumstances of this breach, one of Health PEI's administrative safeguards was not actually implemented. Safeguards are not only used to prevent breaches, but are also used to minimize the personal health information which may be at risk. This minimization of risk is consistent with subsections 39(1) and (4) of the *HIA*, set out above. In this case, an established technical safeguard was not put to use. Health PEI advises that in April, 2014, the QEH Human Resources office was notified by the LPN Association of PEI of the names of all LPNs who chose not to complete the new licensing requirements. The Employee's position changed from LPN to PCW. However, the process for changing access to the CIS is separate from the Human Resources process, and is administered by Information Technology Shared Services ("ITSS"). Management is responsible for submitting an ITSS Employee Change Request Form to ITSS. In this case, no request to change the scope of personal health information available was submitted. For the ensuing years, the Employee kept their LPN credentials to sign into the CIS.

This again demonstrates the importance of collaboration and robust processes that consider all consequences of change. The report does note, at paragraph 21, that,

> Once it was determined that the Employee had accessed the CIS without authorization, Health PEI immediately revoked the Employee's access to personal health information, and cancelled all of the Employee's scheduled shifts.

The above examples from reports emphasize the importance of having robust policies and procedures that require communication and collaboration with various divisions and personnel in an entity when investigating potentially inappropriate access.

PHIA Privacy Breach Statistics November 1, 2025 – January 31, 2026

Between November 1, 2025 and January 31, 2026, OIPC received 10 privacy breach notifications, which is an increase over last quarter's two breaches. The 10 breach reports came from five different custodians. Five breaches involved issues with mailouts, one a misdirected email and one was intentional. Three breaches involved cybersecurity matters and were reported by companies with patients in Newfoundland and Labrador, however with main offices in other provinces.

Want Training?

We would like to remind custodians that OIPC offers PHIA training that can be customized to their needs. We are available to speak at annual general meetings and other events on a variety of access and privacy topics pertinent to custodians.

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

There are also a number of PHIA resources available on OIPC's website.