SAFEGUARD

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

Volume 10, Issue 3 August 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

Instagram:
@oipcnl

YouTube:
@OIPCNL

Blue Sky:
@oipcnl.bsky.social

This Issue:

OIPC Updates

PHIA Review

On June 26th, Premier Wakeham released a statement announcing an immediate review of the Personal Health Information Act and other relevant legislation. On September 1st, the Department of Health and Community Services launched public engagement to inform the 2026 PHIA Review. OIPC encourages all interested parties to engage in the process and have their voice heard.

New Guidance – AI Scribe

OIPC has published two new pieces of guidance: AI Scribe PHIA Guidance and a companion piece, a fillable Word document called AI Scribe Self-Assessment. Both documents can be accessed on our PHIA Guidance page under the privacy tab.

The guidance is intended to assist custodians who are using, or are considering using, Artificial Intelligence (AI) scribe technologies. While the guidance itself is informational in nature, the self-assessment is intended to be completed by the custodian, with details specific to their selected tool to better ensure compliance with the requirements of PHIA.

Instagram

OIPC is expanding our social media presence! The OIPC NL Instagram account (@oipcnl) is active and we invite custodians to bookmark and follow us.

Feedback

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

Privacy in Practice: Adoption of Artificial Intelligence (AI)

This is a new column, created in response to feedback gathered during OIPC's recent survey on our guidance, newsletter and conference. This column will present a scenario and identify PHIA considerations; it is hoped that this will help custodians in their everyday work. If you have a scenario you would like to see featured, let us know by emailing commissioner@oipc.nl.ca with the subject "PHIA Scenarios."

Scenario: I am a custodian considering using Artificial Intelligence, such as an AI Scribe, in my practice. What should I consider?

AI solutions, such as an AI Scribe, are gaining popularity among custodians, as they promise efficiencies and other benefits. But what should custodians consider before adopting such technologies?

AI solutions collect, use, and disclose information; sometimes AI solutions introduce new uses and disclosures, for example using information to train the solution. The collection, use, disclosure, retention, and disposal of personal health information by custodians in this province is governed by PHIA. Custodians that decide to use an AI solution must ensure they have legal authority for the purpose for which they want to collect, use, and disclose the personal health information in the system, and that these activities comply with PHIA requirements.

Up front, custodians should clarify their relationship with providers of AI solutions in the context of PHIA. Are they an agent, information manager, or something else? A key consideration for agent is whether the vendor acts only for or on behalf of the custodian and not the agent's purpose. For example, will the vendor use the information for training purposes? On the other hand, information managers process, retrieve, store or dispose of personal health information, or provide information management or information technology services to custodians, and require an agreement under section 22 of PHIA.

Other considerations include revisiting current processes, policies, and communications materials to determine if modifications are required to reflect the new AI solution. For example, how will you inform patients about the use of the AI solution? Will you ask for consent prior to using the solution or disclosing patient information to the AI solution? What process will be followed if a patient declines to consent?

Custodians need to select technologies they can trust and to do this they must understand the tool, including its functionality, safeguards and limitations. OIPC has developed guidance on AI Scribe; while specific to AI Scribe tools, the same considerations apply to the adoption of any AI solution. Ontario's IPC and Human Rights Commission issued Joint Principles for Responsible Use of Artificial Intelligence that may also be of value.

Report PH-2026-001 Released: Recommended Naming the Snooper

On August 10th, OIPC released Report PH-2026-001. This report details a snooping breach that occurred when a registration desk employee deliberately searched for and viewed the

Complainant's health information. This action was unauthorized because it was not a function of the employee's roles and responsibilities with NLHS and the employee was not part of the Complainant's circle of care as set out in section 24 of PHIA.

The NLHS investigation revealed that the intentional privacy breach was motivated by personal reasons of the employee. The health information obtained by snooping was disclosed to a member of the public known personally to both the employee and the Complainant, leading to the conclusion that this shared health information resulted in harm to the Complainant, including emotional and physical distress.

NLHS investigated the breach, running an access audit of the complainant's health record, following up with the employee who committed the breach, and taking steps to prevent further access by the employee to the Complainant's records. NLHS had a number of safeguards in place at the time the breach occurred, including requiring the employee to take an Oath/Affirmation of Confidentiality and complete privacy education, notably the PHIA online education course. In response to this breach, NLHS's privacy department issued memos, guidance, and reminders across the organization. NLHS's Chief Privacy Officer issued a memo about inappropriate access to records – snooping - and the NLHS Privacy and Access to Information Matters newsletter also includes short articles and reminders on a variety of privacy related topics such as release of medical records, privacy breaches, and privacy/access audits.

The report concluded that a privacy breach occurred when the employee of the Custodian, without consent or appropriate authority to do so, accessed, and subsequently disclosed, the Complainant's personal health information. The Complainant maintains the employee accessed their health information with the intent to cause them harm, and holds the position that the employee should be named publicly and charged. The report examined considerations relating to the disclosure of the employee's name by the Custodian to the Complainant.

OIPC recognizes that affected individuals are in the best position to understand the impacts of the privacy breach upon themselves. This is facilitated by knowing the identity of the snooper, information which would need to be disclosed by the Custodian. The report recommends all custodians develop and implement a privacy breach notification policy that addresses snooping specifically. For any custodian that is also a public body subject to ATIPPA, 2015, the policy should consider the application of section 40(5) of ATIPPA, 2015 to determine if employment status or disciplinary measures are an unreasonable invasion of personal privacy. The policy should recognize that the identity of the snooper may impact the affected person's ability to understand the nature and scope of the breach, assess harm, determine any ongoing risk to their privacy or safety, and make informed decisions on any steps they may wish to make. Section 40(5) requires an assessment of all relevant circumstances, so having a policy to guide the decision-making process will be helpful to ensure clarity. It is also necessary for a custodian to determine through an investigation, the relationship of the parties, to assess harm as part of the notification process. In a situation as was present in NLHS's investigation, the relationship of the parties, which may suggest the motivation behind the unauthorized access, can be an important factor in assessing the risk of harm.

The report concluded with a recommendation that NLHS make a full notification to the affected person including the snooper's name and the discipline they received as a result of this incident, within 60 days of receiving OIPC's report.

Vulnerable People

In the November 2022 edition of Safeguard, then Commissioner Harvey penned a message about dignity, respect and privacy of vulnerable people. At the time, it was in response to breach reports regarding individuals working in healthcare taking pictures of clients at their most vulnerable. Some of these pictures were shared, either among individuals or publicly. This issue is back in the media, with a recent decision by the Newfoundland and Labrador College of Nurses after an investigation into one of their members and their role in such a situation.

While legislation such as PHIA, the **Adult Protection Act** and the **Children, Youth and Family Act**, provide a broad framework for the protection of vulnerable minors and adults, they must be viewed in conjunction with common sense, respect and basic human decency. Anyone of us can find ourselves in a vulnerable situation. We all have a role to play in ensuring the best possible outcome

PHIA requires custodians to have reasonable safeguards in place to protect personal health information. The purpose of the Act establishes rights of individuals and accountabilities for custodians. PHIA also requires that custodians develop policies and procedures to support compliance with the Act. If you are an employee in the health sector and you're unsure about whether there are policies for you to follow, you should contact your employer.

PHIA Privacy Breach Statistics May 1st – July 31st

Between May 1 and July 31, 2026, OIPC received eight privacy breach notifications, which is an increase over last quarter's five breaches. The eight breach reports came from three different custodians. Three breaches occurred when the incorrect file was pulled; custodians are reminded of the importance of confirming they have selected the correct file before making any changes or creating requisitions. One breach occurred when the client provided the incorrect fax number and another when a correctly addressed letter was delivered to a different address.

Two breaches involved abuse of access to medical records. One snooping incident was picked up during an access audit. The second incident was reported by a member of the public who was in receipt of screen shots of medical records containing patient information after an employee sent them.

Custodians are reminded that OIPC will only be accepting privacy breach reports that are sent using the official OIPC Privacy Breach Reporting Form. All other reporting forms will be rejected, and the custodian will need to re-submit. Additionally, custodians are reminded that personal health information should not be included in the breach reports submitted to this Office.

As well, please 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.

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.