OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report PH-2026-001

August 10, 2026

Newfoundland and Labrador Health Services

Summary: The Complainant notified Newfoundland and Labrador Health Services that an employee had breached their privacy. An audit of the complainant's health record found the employee accessed the Complainant's records on one occasion. Newfoundland and Labrador Health Services conducted an investigation and provided the affected person with a breach notification and informed them of their right to submit a privacy complaint to this Office. The Commissioner found that NLHS had adequate protections in place, contained the privacy breach, and provided appropriate notice to the affected individual upon discovery of the breach. The Commissioner found that NLHS took appropriate steps to prevent a future breach from occurring. The Commissioner recommends, in the event of a snooping related privacy breach, custodians and public bodies seriously consider providing affected individuals with the name of the snooper.

Statutes Cited: Personal Health Information Act , SNL 2008 c. P-7.01 sections 5, 15,

Access to Information and Protection of Privacy Act, 2015, SNL 2015, c A-1.2 section 40.

Authorities Relied On: ON OIPC Reports IPC Order HO-010

PEI OIPC Breach Report HI-18-005

SASK OIPC Investigation Report 203-2019, 214-2019, 257-2019

BACKGROUND

[1] In October 2025, the Complainant notified Newfoundland and Labrador Health Services ("NLHS" or the "Custodian") that an employee had breached their privacy. The breach involved an allegation of snooping by an employee who held a registration desk position at a hospital. An access audit of the complainant's health record found the employee accessed the Complainant's records on one occasion. The employee's access to the Complainant's record 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 the Personal Health Information Act (PHIA).

[2] NLHS followed up with the employee who committed the breach. Steps were taken to prevent further access by the employee to the Complainant's records. NLHS determined that the breach resulted from the actions of one employee for their own personal reasons, despite having taken an Oath/Affirmation of Confidentiality and completed privacy education, notably the PHIA online education course. The employee no longer works with NLHS.

[3] NLHS contacted the Complainant to provide the facts of the breach, share an audit report listing all access by the employee to their health record, and convey apologies for the breach.

[4] After the discovery that an employee had accessed and used personal health information without legal authority, the Custodian informed the patient of their right to contact the Office of the Information and Privacy Commissioner.

[5] The patient filed a privacy complaint with the OIPC under the Personal Health Information Act ("**PHIA**").

[6] As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 67(2) of the Act.

CUSTODIAN RESPONSE

[7] NLHS acknowledges that unauthorized access to the Complainants' health information occurred and this access constituted a privacy breach under PHIA. NLHS maintains it acted quickly to investigate in accordance with PHIA and its internal privacy breach policy. Specifically, through an audit of access to the Complainant's health record, NLHS found: 1) that the employee accessed the Complainant's records, and 2) the employee's access to the Complainant's record was unauthorized because it was not a function of the employee's roles and responsibilities with NLHS.

[8] NLHS advises that this breach resulted from the actions of one employee for their own personal reasons, despite having taken an Oath/Affirmation of Confidentiality and completed privacy education. It also confirmed that the employee no longer works for NLHS.

[9] NLHS took steps to prevent further access by the employee to the Complainant's records. NLHS maintains it responded appropriately to the breach, investigated the incident, and took measures to reduce the likelihood of a similar occurrence.

[10] In response to this breach, NLHS's privacy department issued memos, guidance, and reminders across the organization. Concerning the subject of this complaint, NLHS's Chief Privacy Officer issued a memo about inappropriate access to records – snooping. 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.

COMPLAINANT'S POSITION

[11] The Complainant submits that a privacy breach occurred, causing them harm, including emotional and physical distress. The Complainant maintains the employee accessed their health information with the intent to cause them harm. The Complainant holds the position that the employee should be named publicly and charged.

DECISION

[12] The evidence demonstrates that the employee deliberately searched for and viewed the Complainant's health information, knowingly disregarding their responsibilities under the Act, and the Custodian's policies regarding privacy and confidentiality.

[13] The NLHS investigation revealed that the intentional privacy breach was motivated by personal reasons of the employee. Additionally, this Office established that the health information obtained through unauthorized access was subsequently used against the Complainant.

[14] The health information obtained by snooping was disclosed to a member of the public known personally to both the employee and the Complainant. The evidence leads to the conclusion that this shared health information resulted in harm to the Complainant. The Complainant asserts the sharing of this health information was done with the intent to inflict both physical and emotional harm.

[15] There is no question in this circumstance that a privacy breach occurred, an employee of the Custodian, without consent or appropriate authority to do so, accessed, and subsequently disclosed, the Complainant's personal health information. The issue to be discussed in this report is the disclosure of the employee's name by the Custodian to the Complainant.

[16] OIPC PEI released Breach Report HI-18-005. The Report states, in part:

> In most circumstances individuals who interact with a health care provider should know who is accessing their personal health information. In cases of CIS snooping, affected individuals have a heightened need to know the identity of the snooper, for various reasons, but primarily to identify whether the snooper is someone with malicious intentions. The Commissioner recommended that, for any future cases of CIS snooping, Health PEI should proactively provide a copy of an excerpt of the log of accesses to an affected party's electronic personal health information on the CIS, highlighting the dates(s) and the name of the snooper.

[17] As highlighted in Saskatchewan's Investigation Report 203-2019, 214-2019, 257-2019 it is often necessary for the custodian to determine the relationship between the individuals

in order to assess the potential harm to the affected individual. At para 68, the Saskatchewan Information and Privacy Commissioner states,

> My office's position is that an individual who has snooped should have a diminished expectation of privacy. Their identities and the disciplinary action taken against them should be revealed to affected individuals. The impact of a privacy breach is not standard and flat. Learning that a best friend, business partner, estranged spouse, co-worker, boss, neighbour, or a stranger snooped upon one's personal health information has different implications for individuals. Affected individuals are in the best position to understand the impacts of a privacy breach upon themselves. Knowing the identity of the snooper provides affected individuals with information to assess the harm that may result from having their privacy invaded. In my Investigation Report 100-2015, I cited the former Ontario Information and Privacy Commissioner's Investigation Report HO-010 that provided that aggrieved individuals have a right to a complete accounting of what has occurred. Aggrieved individuals will not find closure regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required. Further, publicly identifying the snooper and the disciplinary action taken against the snooper would be a strong deterrent for other employees and contractors.

[18] Ontario Information and Privacy Commissioner's Investigation Report HO-010 provided:

> This level of transparency is important for several reasons. Accessing a patient's personal health information in an unauthorized manner is a serious violation of an individual's privacy and security of the person. In such a situation, the aggrieved individual has a right to a complete accounting of what has occurred. In many cases, the aggrieved parties will not find closure regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required.
>
> For other staff members of the hospital involved, knowing that all of the details of the disciplinary action imposed will be publicly disclosed, should serve as a strong deterrent.

[19] This Office shares the view 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.

[20] Furthermore, this Office asserts that Custodians should be naming the snooper, as it is part of the personal health information of the person who was snooped upon and therefore,

they have a right to that information. The relevant portions of the definition of “personal health information” as set on in 5(1) of PHIA are:

> 5.(1) In this Act, "personal health information" means identifying information in oral or recorded form about an individual that relates to
>
> ...
>
> (b) the provision of health care to the individual, including information respecting the person providing the health care;
>
> (d) registration information;
>
> ...
>
> (g) information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;

[21] Custodians should 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.

[22] It is also necessary for the Custodian to determine through the investigation, the relationship of the parties, to assess harm as part of the notification process. In a situation as is present in this 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.

[23] We have considered whether additional safeguards could have reasonably prevented the snooping incident. The breach resulted from the deliberate decision of one employee to disregard the Act and the privacy program requirements of NLHS for personal reasons.

[24] PHIA requires that custodians implement reasonable safeguards to protect privacy. There is no evidence of a deficiency in the Custodians privacy program that could have led or contributed to this breach.

[25] The Custodian met its obligations under section 15 of PHIA by implementing appropriate policies, informing staff of those policies, and ensuring that staff took an oath of confidentiality that they would abide by those policies. The Custodian also met its obligations in responding to and investigating the incident. NLHS acknowledged the breach and confirmed the employee no longer works for NLHS. While the employee snooped with intent and caused harm, the Custodian fulfilled its statutory obligations under PHIA and as such this Office has no recommendations requiring additional administrative or technical safeguards.

[26] Having considered the circumstances of this case and the procedural history of similar matters in the past, the Commissioner has decided not to pursue prosecution of the Employee under s. 88 of the Act.

RECOMMENDATIONS

[27] Pursuant to section 72(2)(c)(iv) and (d) of the Personal Health Information Act I recommend that:

- Newfoundland and Labrador Health Services 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 this Report.
- NLHS consider implementing an information practice of informing affected individuals of the names of individuals who intentionally access their personal health information in contravention of the Act.

[28] As set out in section 74 of the Personal Health Information Act, Newfoundland and Labrador Health Services must give written notice of its decision with respect to these recommendations to the Commissioner and to any person who was sent a copy of this Report within 15 days of receiving this Report.

[29] Dated at St. John's, in the Province of Newfoundland and Labrador, this 10th day of August 2026

Kerry Hatfield
Information and Privacy Commissioner
Newfoundland and Labrador