

Investigation Report IR23-01 - Nova Scotia Health Intentional Employee Privacy Breaches Background and Report Summary

This document accompanies and summarizes Investigation Report IR23-01. For full facts, findings, and recommendations please refer to the complete report.

Why the OIPC did this investigation

Following the tragic mass casualty event that took place in Portapique, Nova Scotia, on April 18-19, 2020, Nova Scotia Health (NSH) proactively monitored its employees' access to the electronic health records of individuals involved in or related to the tragedy. NSH found that eight employees had used their access to electronic health information systems to intentionally look at these individuals' electronic health records without an authorized work-related reason to do so. This behaviour, commonly known as "snooping", occurs when someone uses the personal information that they have access to for work purposes for their own personal purposes. It doesn't matter if it is done out of curiosity, concern, or for personal gain – it is snooping. Snooping is a privacy breach under Nova Scotia's *Personal Health Information Act (PHIA)*.

As part of its investigation, NSH conducted additional audits of these employees' access to electronic health records which revealed even more breaches going back for years.

NSH voluntarily reported these privacy breaches to the Office of the Information and Privacy Commissioner (OIPC) on June 15, 2020. Given the concerning nature of these unauthorized accesses to electronic health records, the Commissioner started her own investigation into NSH's response to the privacy breaches (s. 92(2)(b) of *PHIA*).

Investigative process

OIPC investigators obtained and reviewed copies of NSH's audit reports, policies, and procedures. The steps NSH took to investigate and respond to these privacy breaches were also reviewed. OIPC investigators interviewed and obtained written statements from NSH's Privacy, Human Resources, and Information Technology Offices, and also heard from individuals who were affected by the privacy breaches. The eight employees who did the snooping were invited to provide their side, but only one agreed to an interview.

How many people were affected by these privacy breaches?

In total, the eight employees snooped on 270 individuals more than 1200 times.

Key findings

The Commissioner made 12 findings. A summary of the key findings is provided below:

- There is room for improvement of the content of NSH's institution-wide privacy training and its practices for ensuring training takes place annually.
- NSH's role-based access practices are not strong enough. Too many employees have access to information they don't need to see.

- NSH did not consistently follow its own policies and procedures when responding to these privacy breaches.
- NSH has not dedicated enough resources to proactively audit and monitor potential snooping by employees.
- There is room for improvement in NSH’s privacy management program and in fostering an internal culture of privacy.

Key recommendations

The Commissioner makes 12 recommendations. A summary of the key recommendations is provided below:

- NSH should strengthen its institution-wide privacy training and its practices for making sure privacy training takes place annually.
- NSH should take steps to limit employee access to detailed personal health information.
- NSH should train staff who are responsible for responding to privacy breaches to follow existing policies and procedures.
- NSH should provide sufficient resources to update and implement its auditing plans for monitoring potential snooping actions by employees.
- NSH should implement stronger leadership and governance (particularly in terms of its privacy management program) to create a culture of privacy.

Nova Scotia Health’s response to the recommendations

NSH is considering the report and has preliminarily indicated that it intends to accept most of the recommendations. NSH will have 30 days to formally decide whether it will follow Commissioner Ralph’s recommendations.

Key take aways

The urge to snoop into individuals’ electronic health records is hard for some employees to resist. That is why it is so important for organizations to have policies that quickly catch snooping, denounce it, and enforce penalties for staff that snoop. NSH has many measures in place, but more can be done to reduce the risk of employee snooping in the future.