# SAFEGUARD

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

Volume 7, Issue 1 February 2023

**Contact Information**

Office of the Information and Privacy Commissioner

3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
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

www.oipc.nl.ca

This Issue:



## Statutory Review of the *Personal Health Information Act*

On February 8, 2023, the Department of Health and Community Services (the Department) announced that the Statutory Review of the *Personal Health Information Act* (*PHIA*) will begin.

*PHIA* establishes rules that custodians of personal health information must follow when collecting, using and disclosing individuals' personal health information.

*PHIA*, proclaimed in 2011, is required to undergo a review once every 5 years and it is intended that this review will result in recommendations to modernize the legislation, including:

- An environmental scan looking at opportunities for improvement and legislation from other jurisdictions;
- Interviews with stakeholders across Newfoundland and Labrador and other provinces and territories; and
- An opportunity for public input.

The Department announced that INQ Consulting and INQ Law, both having a focus on data privacy protection, have been appointed to assist in its statutory review of *PHIA*. A statutory review committee has also been established with representatives from INQ Consulting, INQ Law and officials from the Department. Our Office will also be involved with the review given our oversight role of *PHIA*.

The Department stated that the public will be invited to participate in an online questionnaire through engageNL and anyone who is interested in providing a written submission as part of the review may do so by emailing phiareview@gov.nl.ca.

## Recent Snooping Report from Nova Scotia

Nova Scotia Health experienced intentional privacy breaches when 8 employees accessed the personal health information of 270 individuals more than 1200 times.

The Office of the Information and Privacy Commissioner for Nova Scotia (OIPC NS) conducted an investigation, resulting in Report IR23-01. The following information has been taken from the Background and Report Summary produced by the OIPC NS.

Nova Scotia Health (NSH) proactively monitored its employees' access to the electronic health records of individuals involved in or related to the tragic mass casualty event that took place in Portapique, Nova Scotia, on April 18- 19, 2020. 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 well as under Newfoundland and Labrador's *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 those privacy breaches to the OIPC NS on June 15, 2020. The Commissioner started her own investigation into NSH's response to the privacy breaches (s. 92(2)(b) of *PHIA*).

OIPC NS investigators obtained and reviewed copies of NSH's audit reports, policies, and procedures. The steps NSH took to investigate and respond to the privacy breaches were also reviewed. OIPC NS 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.

### A Summary of the Key Findings from the Commissioner:

- 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.

**A Summary of the Key Recommendations from the Commissioner:**

- 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.

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.

## Tips for Addressing Employee Snooping

The Office of the Information and Privacy Commissioner for Newfoundland and Labrador (OIPC) gratefully acknowledges that the following guidance is based on the work of:

- Office of the Information and Privacy Commissioner for Nova Scotia Tips for Addressing Employee Snooping.pdf (novascotia.ca); and
- Office of the Privacy Commissioner of Canada Ten tips for addressing employee snooping - Office of the Privacy Commissioner of Canada

**Educate**

1. Foster a Culture of Privacy

   An organization's culture of privacy is perhaps the most important element in the prevention of employee snooping, as it supports the effectiveness of all other measures. Visible support from senior leadership is necessary when advancing a culture of privacy. Establish clear expectations and requirements for employees through comprehensive privacy policies and procedures. Operationalize the privacy policies and procedures in practices to ensure employees (i) understand that privacy is a core organizational value, and (ii) know what it means for their day-to-day activities. Privacy policies and procedures are simply documents unless they are implemented effectively and resourced and monitored appropriately. Give your organization's privacy officer (or similar role) a clear mandate and sufficient resources to educate, monitor compliance, and investigate and address violations. When the importance of, and the practices associated with respecting privacy are front-of-mind, employees are less likely to snoop without thinking. This helps to avoid incidents based on impulsiveness, misunderstanding or curiosity.

2. Have Periodic and/or "just-in-time" Training and Reminders of Policies Around Snooping

   Employees are often presented with their privacy obligations as part of a large orientation package upon hiring. While this is good practice, it should not be the only time such policies are presented to employees. Regular reminders and training will ensure knowledge remains fresh.

Effective training content is also important. For example, health custodians should train their employees that snooping is a prosecutable offense under PHIA. Where possible, an organization can use a "just-in-time" reminder, such as a computer pop-up, to present key information about employees' privacy obligations at precisely the time it may be needed.

3. Ensure Employees Know the Consequences will be Enforced

Whether it is curiosity, a request from another person, or even the lure of financial or another type of gain, some employees may have an incentive to snoop. It is up to organizations to ensure their employees are aware that there are serious repercussions for doing so. Employees should understand that:

- There are significant consequences and damages that can arise from snooping.
- The organization takes steps to detect and dissuade violators.
- The organization will enforce consequences.

The absence of any of these three factors will negatively impact the effectiveness of the organization's snooping prevention measures. Having employees sign (upon hiring and at regular intervals) confidentiality agreements that speak to both unauthorized access to, and disclosure of, personal information or personal health information can contribute to creating this awareness.

**Protect**

4. Ensure Access is Restricted to Information Required to Perform the Job

An employee's access to information should be matched to their role so that their access is limited to what they need to know to do their job. This might mean, where feasible, they can only access less sensitive portions of the information about an individual. It may also mean that the employee can only access information about a limited number of individuals and/or groups. Organizations should also have documented processes in place for granting and revoking access to information, as required (such as when an employee changes roles). Particularly where information is sensitive, organizations should use physical (e.g., locked cabinets), administrative (e.g., appropriate policies and consequences) and/or technological (e.g., restricted access permissions) safeguards to prevent unauthorized access to information.

5. Allow Individuals to Block Specific Employees from Accessing their Personal Information

Situations may occur where individuals have a legitimate interest in preventing one or more employees of an organization (e.g., family members, co-workers or ex-partners) from accessing the individual's personal information or personal health information. Organizations should have measures in place to accommodate these requests. To ensure adequacy, the blocked employee should not be able to circumvent this measure.

6. Have Access Logs in Place

Unauthorized access may not be immediately visible. Incidents may come to light over time or as the result of a complaint from an individual. Having access logs that capture when an employee views personal information or personal health information is critical. It means that an organization is better able to investigate allegations of employee snooping, as reviewing the logs can help confirm/deny employee snooping allegations against an employee. Making employees aware that these oversight measures exist also plays a role in deterrence. If employees realize

there is a high probability of being caught, the likelihood that they will engage in snooping in the first place can be significantly reduced.

### Monitor

7. Proactively Monitor and/or Audit Access Logs

It is important that organizations have proactive measures in place to monitor and/or audit access logs for undetected employee snooping. Such measures are essential safeguards to detect and deter unauthorized access by employees, and are particularly crucial for organizations that, for specific operational reasons, must permit employees broader access to personal information or personal health information. Conducting regular audits, random audits or targeted audits are all helpful in identifying unauthorized access. Auditing software is a critical tool needed to support proactive auditing. To maximize deterrence, employees should be made aware that these proactive steps will take place. Without the potential for proactive detection, incidents of employee snooping could continue indefinitely without the knowledge of the affected individual(s) or the organization.

8. Understand "normal" Access, to Better Deter Inappropriate Access

An employee accessed the personal information of a particular person 10 times in one week, or once a week for a year. Another has accessed 9000 different files once each over a two-year period. Are either of these behaviours indicative of a problem? Organizations should understand baseline access patterns for various roles to better detect anomalies of access. Alerts can then be set up to notify the organization of potential problematic behaviour.

### Respond

9. Investigate all Reports of Employee Snooping

Due to their potential seriousness, allegations of employee snooping must be taken seriously and investigated properly. By default, an employee's access to all personal information or personal health information should be suspended throughout the investigation. When there is a snooping incident, we will expect the respondent organization to be able to demonstrate that it has undertaken a thorough and timely investigation of any substantive allegations. We will also expect that it has taken the appropriate steps to address any unauthorized access by the employee, mitigate current or future harms to the affected individual(s) and reduce the likelihood of reoccurrence (e.g., revising policies, strengthening safeguards, increasing monitoring or similar measures).

10. Where Proactive Measure Fail, Respond Appropriately

There may be circumstances in which no reasonable proactive measures would have been able to prevent or detect an employee snooping incident. In these instances, it is critical that the organization responds appropriately. This can include, but is not limited to, appropriate consequences for the snooper (which may include disciplinary action), notification to an oversight body and notification to the affected individual(s). Notification to the affected individual(s) must include sufficiently detailed information (e.g., duration, scope and nature of the personal information accessed) to allow the individual(s) to take appropriate steps to mitigate any potential impacts of the incident. In appropriate cases, custodians should also consider whether a prosecution can be initiated under *PHIA*.

### Conclusion

Organizations must ensure they are compliant with their legal obligation to protect personal information and personal health information from unauthorized use. Employee snooping poses a serious privacy risk that if left unchecked can cause significant and lasting reputational and financial damage to affected individuals and organizations. By taking multiple steps to address this risk, including the adoption of practices outlined above, organizations can better protect personal information and personal health information from internal threats.

## Reminder *PHIA* Compliance Checklist for Custodians

A reminder to custodians of the OIPC's *PHIA* Compliance Checklist for Custodians. This 1 page checklist is a quick overview custodians can use or review to ensure that they are complying with the legislation.

As *PHIA* requires personal health information be protected, here are some reminders from our guidance that custodians can implement:

- Administrative Safeguards – these consist of approved written policies, procedures, standards and guidelines that protect patient, employee, and business information.
- Technological Safeguards – these consist of controlling access to and use of technology such as firewalls, password use, encryption of mobile devices, account restrictions and monitoring.
- Physical Safeguards - these consist of physical measures such as locked filing cabinets, keeping computer terminals and white boards away from public areas, and restricting access to unauthorized personnel.

Under *PHIA*, individuals have a right of access to their own personal health information. *PHIA* sets out the requirements for custodians when providing access to the information (section 60) and in limited circumstances refusing access to the information (section 58). Individuals also have a right to have their personal health information corrected.

A privacy breach is any collection, use or disclosure of personal health information that is not authorized under *PHIA* (including theft or loss). For example, personal health information may be lost (a patient's file is misplaced), stolen (a laptop computer is taken) or inadvertently disclosed to an unauthorized person (a letter addressed to patient A is actually mailed to patient B). There are also breaches that are intentional, for example, an unauthorized access of patient files by staff.

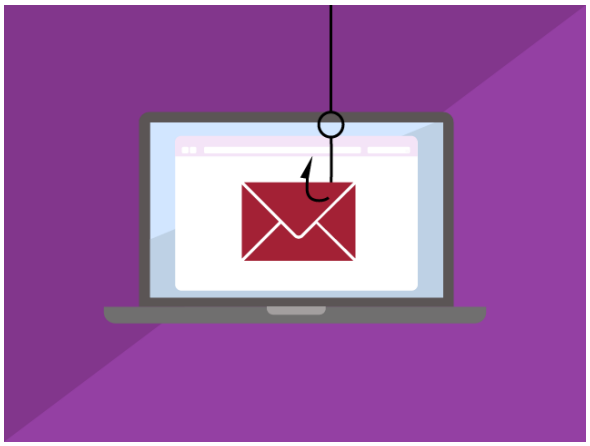
Custodians are responsible for ensuring that any employees, agents, contractors and volunteers are aware of their obligations under *PHIA* and of the policies and procedures that support the legislation.

**New Upcoming Guidance** – Stayed tuned for the OIPC's **Small Custodian Toolkit**

## Breach Notifications

Between November 1, 2022 and January 31, 2023, OIPC received 9 breach notifications from 5 different custodians.

One breach involved a successful phishing attempt, resulting in a threat actor obtaining access to a manager's account. The threat actor was only able to access a limited number of documents, however, the threat actor sent 500 further phishing emails from the manager's account. A number of individuals clicked on the phishing emails, even though almost all had completed mandatory cyber-security training. The manager's account was locked as soon as the problem was detected and in the end only 4 individuals were affected. This breach serves as a reminder that individuals need to continue to be vigilant as emails from a "known" account, like the manager's account, can still be a phishing attempt.



DON'T GET HOOKED