Tips for Addressing Employee Snooping

Office of the Information and Privacy Commissioner for Nova Scotia
February 8, 2023

Notice to Users

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP*, *MGA* and *PHIA* the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any proposal from a public body, municipal body or health custodian. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Commissioner (Review Officer) will keep an open mind. It remains the responsibility of each public body, municipal body and health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca.

ACKNOWLEDGMENTS

The Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) gratefully acknowledges that this guidance document is based on the work of:

- Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/02_05_d_65_tips/
- Office of the Manitoba Ombudsman: https://www.ombudsman.mb.ca/uploads/document/files/ten-tips-for-addressing-employee-snooping-en.pdf

TIPS FOR ADDRESSING EMPLOYEE SNOOPING

The public entrusts significant amounts of personal information and personal health information to Nova Scotian public bodies, municipalities and health custodians (organization(s)).[1] Ensuring this information is accessed only by employees who need it, and only at times that information is required for legitimate work purposes, can be a challenge – but it is a challenge that needs to be addressed. Without appropriate preventative safeguards, human curiosity and other motivations (such as profiting or causing harm to individuals) can cause employees to access this information without authorization and without a legitimate work purpose. This is also known as "employee snooping".

When an employee accesses or views personal information or personal health information, it is a "use" of the information. The *Freedom of Information and Protection of Privacy Act (FOIPOP)*, the *Municipal Government Act (MGA)* and the *Personal Health Information Act (PHIA)* all require that personal information or personal health information not be used except for purposes authorized under the applicable Act. These Acts also require organizations to have reasonable safeguards in place to protect this information from unauthorized use. Although snooping is an unauthorized action of the employee for their own personal purposes, organizations remain accountable for protecting this information from unauthorized use. Below, we provide tips on ways to prevent and address employee snooping.

EDUCATE

1. Foster a culture of privacy.

The most important element in the prevention of employee snooping is an organization's culture of privacy, as it supports the effectiveness of all other measures. Advancing a culture of privacy requires visible support from senior leadership, who set the tone from the top. Establish clear expectations and requirements for employees through a robust privacy management program.[2] Develop a set of comprehensive privacy policies and procedures and operationalize them in

[1] Throughout this guide, the term "organization(s)" will be used to refer to all entities, including public bodies, municipalities and health custodians, that are subject to the *Freedom of Information and Protection of Privacy Act, Part XX* of the *Municipal Government Act* and the *Personal Health Information Act*.

[2] For more information regarding privacy management program requirements, see our suite of guidance documents on this topic: Tools & Guidance | Office of the Information and Privacy Commissioner for Nova Scotia.

concrete practices. This will help 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 respecting privacy and the practices associated with it are front-of-mind, employees are less likely to snoop without thinking. This helps to avoid incidents based on impulsiveness, misunderstanding or curiosity. The organization is also more likely to respond appropriately when a privacy breach caused by an employee snooping is detected, as there would be a common understanding that the employee has contravened a core value of the organization's culture.

2. Have regular and "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 training (e.g., annual privacy training) and reminders 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 that 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 the following:

- 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 employee access is restricted to information required to perform the job.

An employee's access to personal information or personal health 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, that they can only access less sensitive portions of information held about an individual. It may also mean the employee can only access information about a limited number of individuals and/or have other access restrictions in place. For example, access could be limited by time or geography. Pay attention to what search functionality and reports the employee needs. Organizations should also have documented role-based access matrices and processes in place for granting and revoking access, such as when employees change 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. Implement measures that allow individuals to block specific employees from accessing their 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. Under s. 63 of *PHIA*, individuals can also request a record of who accessed their personal health information, i.e., "a record of user activity," free of charge from a health custodian. Health custodians must meet the record of user activity requirements in *PHIA* and its Regulations.

MONITOR

7. Proactively monitor and/or audit access logs.

It is also 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 targeted and focused audits that look for high risk behaviours is key, especially for large organizations. Organizations may also perform random audits or regular audits of all employees. 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 detect 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 this office (OIPC) becomes aware of 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 measures 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 this office (OIPC) 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 contacting law enforcement to explore 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 Nova Scotians' personal information and personal health information from internal threats.

QUESTIONS?

This guidance was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. We encourage organizations to contact us with any questions about this document. Organizations can also consult with our office for free by completing and submitting a Consultation Request Form:

- Consultation Request Guidelines
- Consultation Request Form

Phone: 902-424-4684
Toll Free (NS): 1-866-243-1564
TDD/TTY: 1-800-855-0511
Fax: 902-424-8303
Email: oipcns@novascotia.ca