Ten Tips for Addressing Employee Snooping

Public bodies and trustees hold significant amounts of personal and personal health information about Manitobans in order to provide various services, programs and benefits. Ensuring that this information is accessed only by employees who need it, and only at times that information is required for legitimate work-related purposes, can be a challenge – but it is a challenge that needs to be addressed.

Without appropriate safeguards, human curiosity and other motivations (such as causing some form of harm to individuals and/or trying to gain an advantage) can lead employees to access personal and personal health information without authorization and without a legitimate work-related purpose – also known as "employee snooping."

Access to, or viewing of, personal and personal health information by an employee is considered a "use" of the information. The Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Act (PHIA) require that personal and personal health information not be used (or disclosed) except for purposes authorized under these acts. Both acts require that this information be protected by reasonable safeguards against such risks as unauthorized access, use, disclosure and destruction. Additionally, PHIA requires that the administrative, technical and physical safeguards be appropriate to the degree of sensitivity of the personal health information.

Although snooping represents the unauthorized actions of an employee for their own personal purposes, public bodies and trustees are accountable for their obligations to protect personal and personal health information from unauthorized use or disclosure. Below, we provide tips on ways for public bodies and trustees (organizations) to prevent and address employee snooping.

This privacy guidance has been adapted from *Ten Tips for Addressing Employee Snooping*, prepared by the Office of the Privacy Commissioner of Canada for private sector organizations subject to the Personal Information Protection and Electronic Documents Act (PIPEDA). It has been modified with permission from the Office of the Privacy Commissioner of Canada.

Manitoba Ombudsman

www.ombudsman.mb.ca | ombudsman@ombudsman.mb.ca | 1-800-665-0531 | 204-982-9130

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. Cultivating an organizational commitment to privacy compliance and best practices is most effective when there is visible commitment and support from senior management.

A culture of privacy begins with the establishment of clear expectations and requirements for employees. Develop a set of comprehensive privacy policies and procedures, and reflect and operationalize them in concrete practices, to ensure that employees: (i) understand that privacy is a core organizational value, and (ii) know what this means for their day-to-day activities. Further, give your organization's privacy officer (or a similar role) a clear mandate to educate, monitor compliance, and investigate and address violations. When the importance of, and practices associated with, respecting privacy are front-of-mind, employees are less likely to snoop without thinking – helping to avoid incidents based on impulsiveness, misunderstanding or curiosity.

2 Have periodic and/or "just-in-time" training and reminders of policies around snooping

Quite often, an employee is presented with his or her privacy obligations as part of the orientation package received upon hiring. While this is a good practice, it should not be the only time such policies are presented to employees. Regular reminders and training will ensure knowledge remains fresh. Incorporate practical examples that are relevant to the particular workplace. Further, where possible, an organization can use a "just-in-time" reminder – which can range from a sticker on a cabinet to 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 other type of gain, some employees may feel compelled 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: (i) there are significant consequences to, and damages that can arise from, snooping; (ii) the organization takes steps to detect and deter snoopers; and, (iii) consequences will be enforced. The absence of any of those three factors will negatively impact the effectiveness of an 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 and/or personal health information can contribute to creating this awareness. Organizations with personal health information should be aware that PHIA requires that employees and agents of the trustee sign a pledge of confidentiality.

PROTECT

4 Ensure access is restricted to information required to perform the job

An employee's access to personal and personal health information should be matched to his or her role so that access is limited to the information the employee needs to know to perform job duties. This might mean, where feasible, that he or she can access only less sensitive portions of the information held about an individual and/or only information about a limited number of individuals, that access is time- or geography-limited, and/or other restrictions. 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 (ex: locked cabinets), organizational (ex: appropriate policies and consequences) and/or technological (ex: restricted access permissions) safeguards to prevent inappropriate access to the information.

5 Develop measures to enable blocking of employee access to a specific individual's information

Situations may arise in which an individual has a genuine interest in preventing one or more employees of an organization (ex: family members or former partners with whom a contentious relationship exists) from accessing the individual's personal or personal health information. Organizations should have procedures in place to accommodate such requests to the extent possible, by implementing measures to prevent and/or monitor access by the employee(s). Needless to say, the blocked employee should not be able to circumvent this measure.

6 Have access logs and/or other oversight tools in place

Inappropriate access may not be immediately detected. Incidents may come to light over time, or as the result of a complaint from an individual. Having access logs for electronic information or other oversight tools in place allow an organization to investigate allegations of employee snooping by reviewing such logs in order to confirm/deny employee snooping allegations made against an employee.* Making employees aware that these oversight measures exist also plays a key role in deterrence. If employees realize that there is a high likelihood of being caught, the likelihood that they engage in snooping practices in the first place can be significantly reduced.

MONITOR

7 Proactively monitor and/or audit access logs and other oversight tools

Beyond using access logs to investigate alleged incidents, it is important that organizations have proactive measures in place to monitor and/or audit for undetected employee snooping. Such measures are essential safeguards to deter and detect unauthorized access by employees, and are particularly crucial for organizations that, for specific operational reasons, must permit employees broad access to client or patient information. This can take the form of regular audits of all employees or random ones, where an organization is quite large.* Further, to maximize deterrence employees should be made aware that these proactive steps do take place. Without the potential for proactive detection, incidents of employee snooping could continue indefinitely without the knowledge of the affected individual or the organization.

*Please refer to the specific requirements in PHIA regarding records of user activity and auditing.

8 Understand "normal" access, to better detect inappropriate access

An employee has accessed the personal or personal health information of a particular person 10 times in one week, or once a week for a year. Another has accessed 900 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, in order 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 impact, allegations of employee snooping must be taken seriously. When our office becomes aware of a snooping incident, we will expect an organization to be able to demonstrate that it has undertaken a thorough and timely investigation of allegations and, where warranted, taken appropriate steps to address the unauthorized access by an employee, mitigate current or future harms to the individual, and reduce the likelihood of recurrence (potentially including revising policies, strengthening safeguards, increasing monitoring, or similar measures).

10 Where proactive measures fail, respond appropriately

In circumstances where no reasonable proactive measures would have been able to prevent or detect an employee snooping incident, it is important that the organization respond appropriately. This can include, but is not limited to, appropriate consequences for the snooper (which may include disciplinary action) and notification to the affected individual (including sufficient information, such as duration and scope of access, to allow an individual to take appropriate steps to mitigate any potential impacts of the incident). It may also include notification to our office.

Employee snooping poses a serious privacy risk that if left un-checked can cause significant and lasting reputational and financial damage to the affected individuals and your organization. By ensuring compliance with FIPPA and PHIA and taking the appropriate steps to address this risk, including the adoption of the practices outlined above, organizations can go a long way in advancing their reputation as a privacy-conscious organization, and more importantly, protect Manitobans' information, with which they have been entrusted.

Manitoba Ombudsman
Upholding Your Information Access and Privacy Rights
www.ombudsman.mb.ca | ombudsman@ombudsman.mb.ca | 1-800-665-0531 | 204-982-9130