MANITOBA OMBUDSMAN PRACTICE NOTE

Practice notes are prepared by Manitoba Ombudsman to assist persons using the legislation. They are intended as advice only and are not a substitute for the legislation.

Manitoba Ombudsman
750-500 Portage Avenue
Winnipeg, Manitoba R3C 3X1
Phone: (204) 982-9130 Toll free 1-800-665-0531
Fax: (204) 942-7803
Website: www.ombudsman.mb.ca

PROTECTING PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION WHEN WORKING OFF-SITE

Paper and electronic records containing personal information and personal health information of individuals, such as clients, patients, students, and employees, are more vulnerable to a privacy breach when taken off-site. This may occur when employees make home visits to clients, travel to other work locations, attend meetings off-site, or work remotely from home.

Public bodies and trustees are required to make reasonable safeguards to protect personal information and personal health information of individuals under the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Act (PHIA). Safeguards include creating policies that set out procedures for ensuring the security of the information.

The following best practices should be considered when public bodies and trustees establish or review organizational policies and procedures for removing personal information and personal health information from the workplace. Policies and procedures are most effective when they are designed to meet the unique needs of the work environment, are reviewed to ensure they are up to date, and are regularly communicated with employees.

BEST PRACTICES WHEN WORKING OFF-SITE

Determine which records may be removed from the workplace

Not all records are the same. Different categories of records and types of information contained within records may pose varying levels of risk in the event of theft, loss or inadvertent disclosure.

- Identify which categories of records and types of information may or should never be removed from the workplace.
- For records and information that may be removed from the workplace, determine what authorizations, safeguards, and special handling requirements may be required.

Limit the amount of information removed from the workplace

- Take personal information or personal health information off-site only when necessary (for example, consider whether bringing this information is necessary to accomplish the purpose of the meeting).
- If it is necessary to take personal information or personal health information off-site, take the least amount of information needed to accomplish the purpose (for example, take only the relevant information you require for that day's tasks).
- Take copies of the records when practical, and consider the following measures:
    - Clearly identify the copies and retain them only as long as necessary.
    - If possible, de-identify personal information or personal health information on the copies of the records.
    - Redact any other information that is not required on the copies of the records.
- Determine how to track records and other information removed from the workplace (for example, record when they are removed and when they are returned).

Handling paper and electronic records off-site

- Transport personal information and personal health information in a secure manner, such as in a briefcase with a lock, to avoid loss of information.
- Keep personal information and personal health information with you and under your control when off-site, including during meals, breaks and travel.
- Do not leave personal information and personal health information unattended in a vehicle under any circumstances, even in the trunk. Locking information in any part of a vehicle is not considered a reasonable safeguard. Many privacy breaches have occurred as a result of information being left in vehicles.
- Store personal information and personal health information brought home securely (for example, a locked filing cabinet or briefcase to which only you have access).
- Do not leave personal information and personal health information unattended and unsecured in a hotel room. While hotel rooms may be locked, hotel employees have access to rooms, which means that the information may not be secure. Consider alternatives for where the information may be secured, such as in a room safe or at a local site of your organization.
- Avoid viewing personal information and personal health information in public, such as in a restaurant, airport or other public place. If you must view the information, take precautions to ensure no one else can view it.
- Avoid discussing personal information and personal health information in public.
- If using email, ensure that personal information and personal health information being received or sent is password protected or encrypted.

Mobile devices and removeable storage devices

Information technology tools can assist in ensuring the security of information stored on electronic mobile devices (laptops, tablets, mobile phones) and removeable storage devices (CDs/DVDs, flash drives/USB sticks).

- Identify which information technology tools are available for use (for example, encryption technologies, privacy screens for laptops or tablets, or secure virtual private networks [VPNs]).

- Ensure approved tools are available when needed and that employees have been trained on the use of the approved tools.
- Use both encryption and password protection. Encrypt information stored on electronic devices and removable storage devices. Password protect electronic devices and removeable storage devices.
- When choosing a password, ensure it is complex and long enough that it would be difficult for someone to guess it. Never store the password with or near the electronic device.
- Set electronic devices to automatically lock or log off after a brief period of idleness.
- Log off or shut down laptops or tablets when not using them.
- Store electronic devices and removable storage securely when they are not in use.
- Transfer or delete personal information and personal health information from electronic devices and removable storage as soon as the information is no longer required in that medium for the immediate future.
- If using a personal device, take safeguards to ensure that no personal information or personal health information is saved or stored on the personal device. Password protect the device and ensure it locks after a brief period of inactivity. Log off or shut down the device when not in use. Ensure the personal device is not connected to an unsecured wi-fi network.

If a breach occurs

If personal information or personal health information is lost, stolen or otherwise compromised, immediately notify your supervisor and your organization's access and privacy coordinator or privacy officer. For more information, please see the privacy breach resources available on our website at www.ombudsman.mb.ca/info/privacy-breaches.html.