

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
Web site: www.ombudsman.mb.ca

PROTECTING PERSONAL AND PERSONAL HEALTH INFORMATION WHEN WORKING OUTSIDE THE OFFICE

Employees of public bodies under *The Freedom of Information and Protection of Privacy Act* (FIPPA) and trustees under *The Personal Health Information Act* (PHIA) have obligations to protect personal and personal health information. This includes safeguarding the information against such risks as unauthorized disclosure, accidental destruction, loss and theft.

Records containing personally-identifiable information, such as those concerning clients, patients, students or employees, are more vulnerable to a privacy breach when removed from the office or workplace. This may occur when employees make home visits to clients, travel to other work locations, attend meetings off-site, take work home occasionally or work from home on a regular basis.

FIPPA and PHIA require public bodies and trustees to make reasonable safeguards to protect personal and personal health information (FIPPA s. 41; PHIA s. 18, 19, Regulation 245/97). Creating policies that set out procedures for ensuring the security of the information is a requirement under PHIA and a best practice under FIPPA.

Public bodies and trustees should create a policy for protecting personal and personal health information when working outside the office. A policy should be tailored to the needs of the work environment. Employees need to be aware of the policy and understand it.

This document has benefited from similar publications of the Offices of the Information and Privacy Commissioners of Ontario and British Columbia.

BEST PRACTICES WHEN WORKING OUTSIDE THE OFFICE

The following are some best practices for protecting personal and personal health information when working outside the office. These tips should be considered when establishing procedures or developing a policy for taking personal and personal health information outside the office.

Before you Leave the Office

- Identify which categories of records may, or should never, be removed from the office.
- Ensure that current information technology tools are available to and used by employees.
- Establish a procedure for tracking records/files removed from the office (e.g. signing them in and out).

Limit the Amount of Information you Transport

- Take personal or personal health information off-site only when necessary.
- If you must take personal or personal health information with you, take the least amount possible (e.g. take only relevant records from a paper file or relevant electronic information).
- Whenever practical, only take copies of the records. Clearly identify the copies and retain them only as long as necessary.
- If possible, de-identify the personal or personal health information on the copies of paper records and electronic records.

Technical Measures

- Personal and personal health information in electronic records on laptops, PDAs (Personal Data Assistants) and removable storage media should be encrypted.
- Laptops and other electronic devices such as PDAs, including Blackberrys and Palm Pilots, should be password protected.
- Access to personal and personal health information stored on removable storage media such as floppy disks, CDs or USB storage drives should be password protected. When not in use, removable storage media should be stored securely.
- Choose strong passwords of eight characters or more with a combination of numbers and letters in upper and lower case. Passwords should be changed regularly and should never be stored with the electronic device.
- Log off or shut down your laptop or home computer when not using it. Set the automatic log off to be activated after a brief period of idleness.

Information Handling of Paper and Electronic Records

- Transport personal and personal health information in a secure manner such as in a briefcase or similar container to avoid loss of information.
- Keep personal and personal health information with you and under your control when traveling or working outside the office, including during meals and other breaks. If this is not always possible, store the information securely such as in a locked room or desk drawer.
- When traveling, do not leave personal and personal health information unsecured in a hotel room. Store the information in a room safe or hotel office safe or consider storing them at a local office of your organization.
- Avoid viewing personal and personal health information in public, such as when traveling by plane, bus, train or on public transit. If you must view the information, take precautions to ensure no one else can view it.
- Avoid discussing personal and personal health information in public.

- Avoid discussing personal and personal health information on a cell phone as calls can be overheard and may be intercepted.

Information Handling and the Vehicle

- Personal and personal health information should not be left in a vehicle unless there is no other option. In most situations, it is possible, although perhaps not convenient, to take the information with you.
- If the information must be left in the vehicle, it should be locked in the trunk. If the vehicle does not have a trunk, the information should not be visible. Despite the trunk of a vehicle generally being considered to be more secure than the vehicle interior, locked vehicles and trunks may be broken into or vehicles may be stolen so caution must be exercised.

Information Handling at Home

- If you work from home, store the personal or personal health information in a locked filing cabinet that is used exclusively for work-related records and to which nobody else has access.
- Do not store personal and personal health information on your home computer hard drive.
- If you work from home, your employer should provide a separate phone line and a password controlled voice mail box, if possible.

If a Breach Occurs

- If personal or personal health information is lost or stolen, immediately notify your supervisor and your organization's Access and Privacy Coordinator or Privacy Officer. For more information, see our Practice Notes: *Key Steps in Responding to Privacy Breaches* and *Reporting a Privacy Breach to Manitoba Ombudsman*.