

Privacy Breach Planning and Management: A Municipal Perspective

Manitoba Ombudsman

What is a Privacy Breach?

The improper or unauthorized collection, use, disclosure, retention or disposal of personal and/or personal health information. Such activity is considered “unauthorized” if it is not permitted by FIPPA and PHIA.

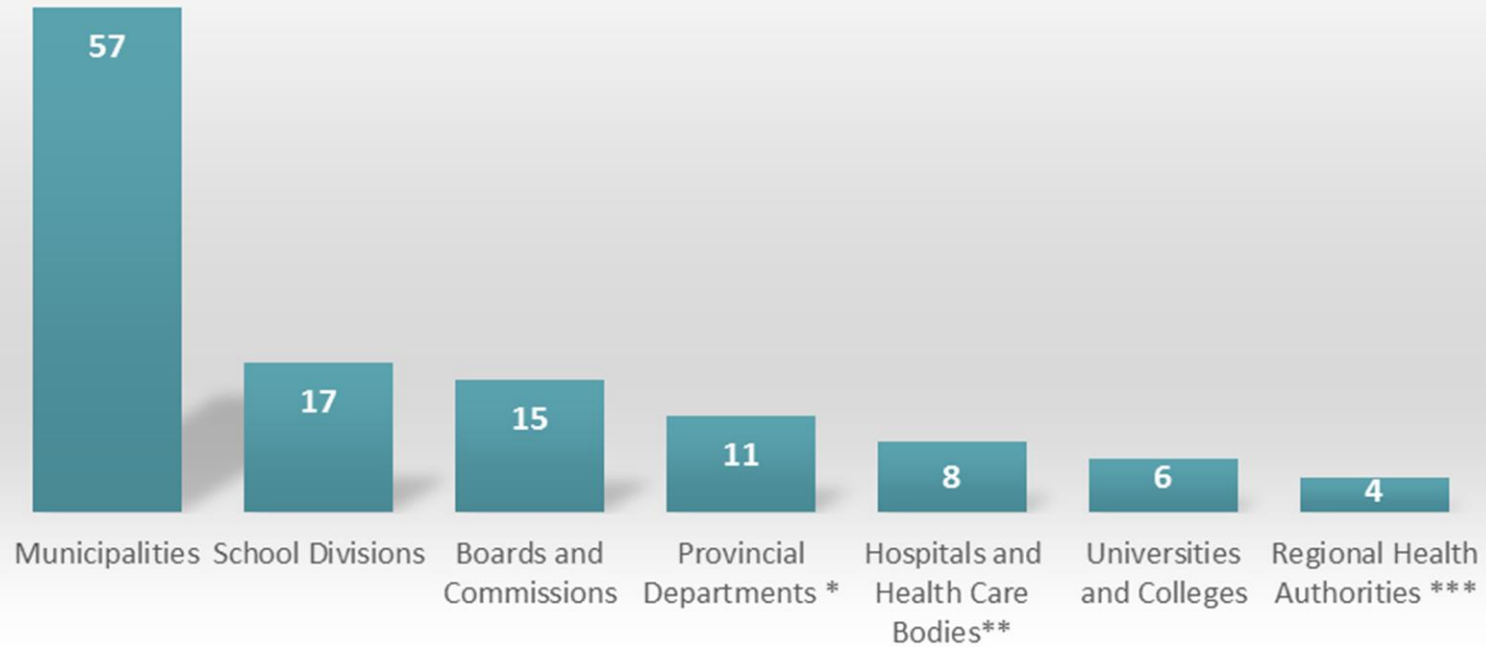
WHY?

In June 2016 our office distributed an electronic survey to 238 organizations, which included:

- © Municipalities
- © School divisions
- © Hospitals
- © Regional health authorities
- © Health-care bodies (that do not fall under an RHA)
- © Boards and commissions
- © Provincial departments
- © Universities
- © Colleges

The Survey

Number of Respondents by Organization



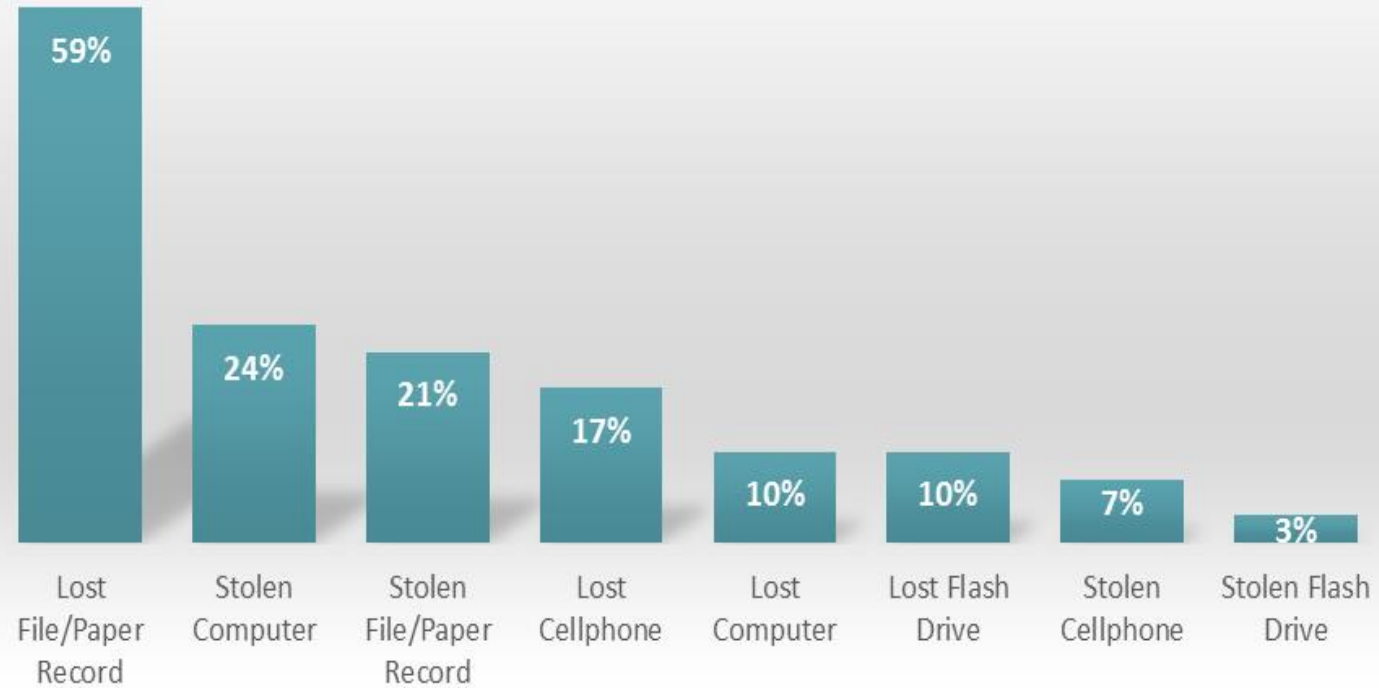
Personal Information? Personal Health Information? Or a Combination of Both?

- © 51% of total respondents indicated that they manage a combination of both personal and personal health information.
- © 23% of municipalities indicated that they manage a combination of both personal and personal health information.
- © The remaining 77% of municipalities responded that they manage only personal information.

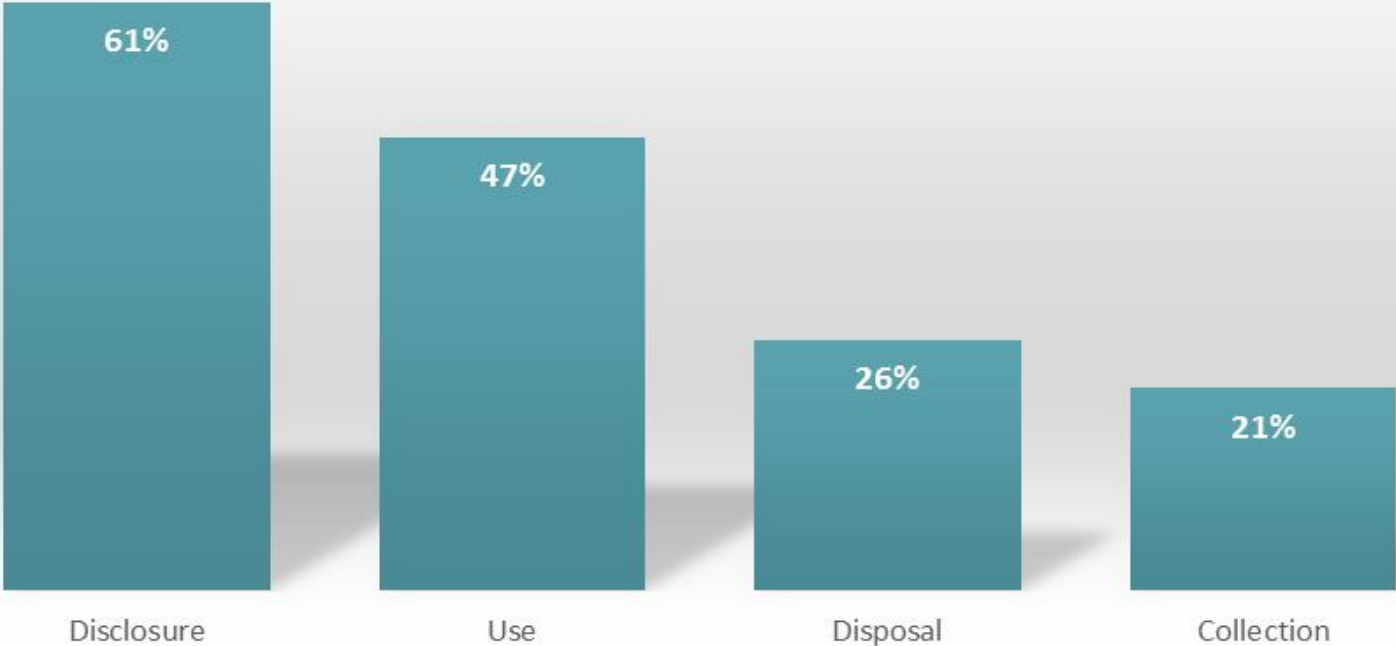
Privacy Breaches

Three of 56 municipalities that responded indicated that they had experienced a privacy breach in the past three years.

Privacy Breach Experienced



Nature of Privacy Breach



Policies Procedures Guidelines

Privacy Breach Training

- © The majority (78%) of total respondents reported that their organization does not provide training specific to privacy breach management.
- © The majority (89%) of municipalities reported that their organization does not provide training specific to privacy breach management.

Internal Reporting

© 72% of total respondents reported that a specific person had been designated to manage privacy breaches in their organization.

© 53% of municipalities reported that a specific person had been designated to manage privacy breaches in their organization which in most cases was the CAO.

Tracking of Privacy Breaches

- © The majority of total respondents (54%) indicated that their organization does not track privacy breaches.
- © The majority of municipalities (77%) indicated that their organization does not track privacy breaches.

Service Agencies and Contractual Obligations

© 26% of total respondents reported that they have contracts with third-party service agencies. Of those, 46% indicated that their contracts or agreements outline the service agency's responsibilities in the event of a privacy breach.

© 18% of municipalities reported that they have contracts with third-party service agencies. Two municipalities reported that third-party contracts contain privacy breach provisions.

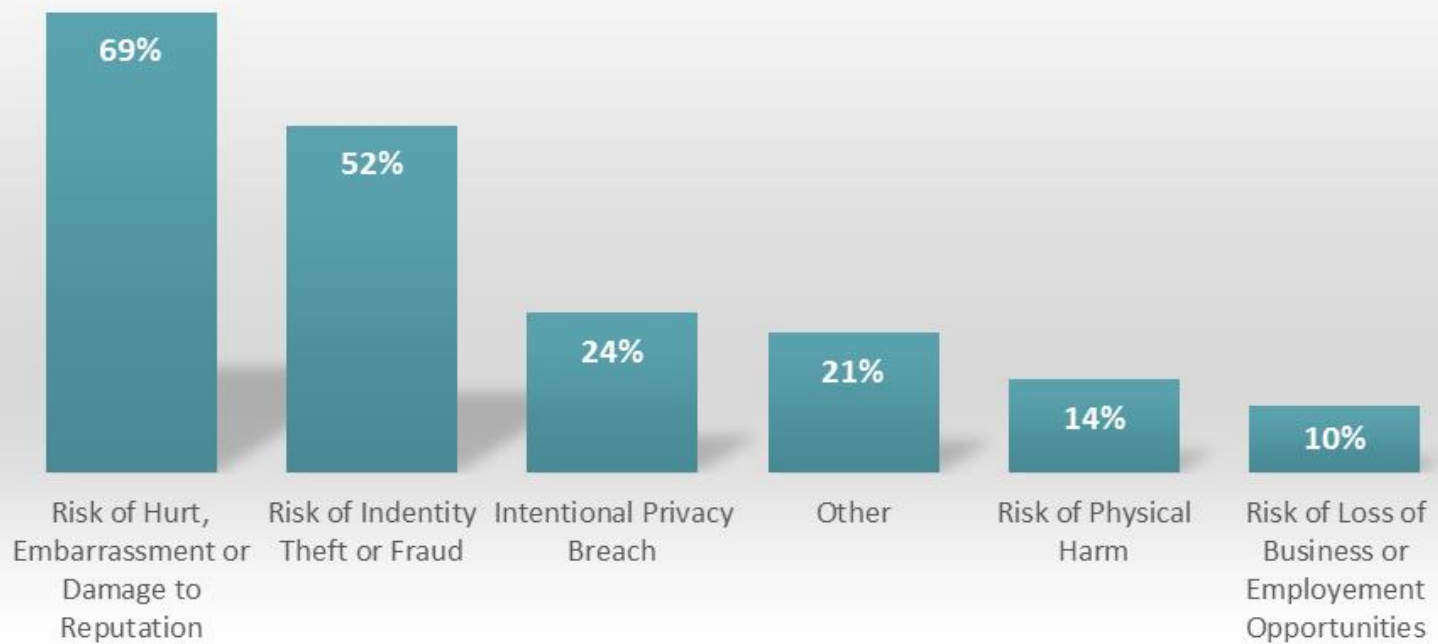
Service Agencies and Contractual Obligations

- © Where privacy provisions exist, 49% of total respondents reported that there is an obligation in their contract to notify the organization when a privacy breach has occurred.
- © Two municipalities reported that there is an obligation to notify the organization in the event of a privacy breach.

Notification

- © 55% of total respondents reported that they contacted Manitoba Ombudsman when a privacy breach occurred.
- © One municipality reported that they contacted Manitoba Ombudsman when a privacy breach occurred.
- © 74% of total respondents reported that they have notified an affected individual as a result of a privacy breach.
- © Two municipalities reported that they have notified an affected individual as a result of a privacy breach.

Reasons to Notify



Resources

© 63% of total respondents indicated that privacy breach training and a sample privacy breach policy would be the most valuable resources.

© 72% of municipalities indicated that privacy breach training and a sample privacy breach policy would be the most valuable resources.

Reducing the occurrence and impact of privacy breaches

What can you do?

- ⦿ Know what personal and personal health information you have
- ⦿ Understand your role under FIPPA and PHIA
- ⦿ Have a designated person to manage privacy breaches
- ⦿ Develop a privacy breach policy
- ⦿ Provide privacy training
- ⦿ Ensure privacy responsibilities are outlined in service contracts
- ⦿ Assess the impact of a breach and consider notification to affected parties
- ⦿ Track and document privacy breaches

New Materials

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 3K1
Phone: 204-982-9150 or 1-800-665-6531
Fax: 204-942-7803
Website: www.ombudsman.mb.ca

KEY STEPS IN RESPONDING TO PRIVACY BREACHS UNDER THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA) AND THE PERSONAL HEALTH INFORMATION ACT (PHIA)


Purpose
The purpose of this document is to provide guidance to public bodies and trustees when a privacy breach occurs.¹

Public bodies and trustees that are developing a privacy breach policy or procedure may find it helpful to incorporate some of this information.

What is a privacy breach?
A privacy breach occurs when there is unauthorized collection, use, disclosure or destruction of personal or personal health information. Such activity is “unauthorized” if it is not permitted by FIPPA or PHIA. The most common privacy breaches happen when personal information about clients, patients, students or employees is stolen, lost or mistakenly disclosed. Examples include when a laptop containing personal or personal health information is stolen or information is mistakenly faxed or emailed to the wrong person.

Reporting privacy breaches
Manitoba Ombudsman has created a Privacy Breach Reporting Form that allows public bodies and trustees to complete an analysis of the privacy breach using the four key steps described below. This form is contained in our practice note *Reporting a Privacy Breach to Manitoba Ombudsman*, and is available on our website.

¹ This document was adapted with permission from *Privacy Breaches: Tools and Resources*, developed by the Office of the Information and Privacy Commissioner (OIPC) of British Columbia, March 2012; *Breach Notification Assessment Tool*, jointly produced by the OIPC of BC and the OIPC of Ontario, December 2008; *Key Steps in Responding to Privacy Breaches and Privacy Breach Report* developed by the OIPC of Alberta, July 2012 and *Key Steps in Responding to Privacy Breaches* developed by the OIPC of Nova Scotia, March 2015.



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”.

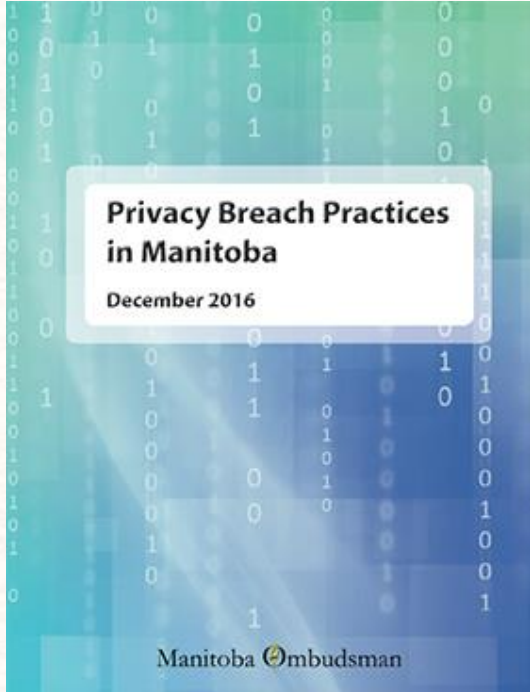
Access to or viewing of personal and personal health information by an employee is considered a “use” of the information. The Freedom of Information and Protection of

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 | 1-800-665-6531 | 204-982-9150



Privacy Breach Practices in Manitoba

December 2016

Manitoba Ombudsman

Privacy Breach Resources: <https://www.ombudsman.mb.ca/info/privacy-breaches.html>

Questions?