



# IMPLEMENTING PRIVACY IN YOUR ORGANIZATION

## A MANITOBA OMBUDSMAN WORKSHOP

Gail Perry

Manager, Research and Education

Nancy Love

Manager, Access and Privacy Division



# WORKSHOP OBJECTIVES

- considering the impact of FIPPA and PHIA privacy provisions on your organization
- exploring case scenarios that help you identify and address privacy considerations
- anticipating where privacy breaches may occur and learning how to mitigate the risks
- looking beyond the legislation and applying best practices in your organization



# ROLE OF THE OMBUDSMAN

The Ombudsman is an independent officer of the Legislative Assembly, who has broad powers of investigation, the ability to recommend corrective action and to report publicly

The Ombudsman's Office was established on the premise that the public should have the right to an independent review of decisions made by government bodies



# OFFICE OF THE MANITOBA OMBUDSMAN

The office has two operational divisions:

The **Ombudsman Division** investigates under:

- ***The Ombudsman Act*** concerning administrative acts, decisions or omissions by any department or agency of the provincial government or a municipal government

The **Access and Privacy Division** investigates complaints and reviews compliance under:

- ***The Freedom of Information and Protection of Privacy Act (FIPPA)*** concerning access to general or personal information and privacy of personal information held by public bodies
- ***The Personal Health Information Act (PHIA)*** concerning access to one's own personal health information and privacy of that information held by trustees

M  
A  
N  
I  
T  
O  
B  
A

O  
M  
B  
U  
D  
S  
M  
A  
N



# WHY PRIVACY MATTERS

M  
A  
N  
I  
T  
O  
B  
A

O  
M  
B  
U  
D  
S  
M  
A  
N

- privacy is a value that affects everyone
- complying with privacy obligations is the law!
- good privacy practice = good business and good administration
- privacy builds and maintains public confidence in the organization



# PUBLIC BODIES UNDER FIPPA

**Provincial Government** (Departments and Government Agencies, Crown Corporations, Ministers' Offices, Executive Council Office)

## **Local Public Bodies:**

- **Local Government Bodies** (City of Winnipeg, municipalities, local government districts, planning districts, conservation districts)
- **Educational Bodies** (school divisions, colleges, universities)
- **Health Care Bodies** (hospitals and regional health authorities)



# TRUSTEES UNDER PHIA

- **Public Bodies** under FIPPA
- **Health Professionals** (licensed or registered to provide health care under an Act or designated in the regulations)
- **Health Care Facility** (hospital, personal care home, psychiatric facility, medical clinic, laboratory, CancerCare Manitoba, and community health centre or other facility designated in the regulations)
- **Health Services Agency** (an organization that provides health care pursuant to an agreement with another trustee)



# RESPONSIBILITY FOR PRIVACY IN AN ORGANIZATION (FIPPA)

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

## Head of a Public Body

- Minister of a department, CEO of a government agency
- person or group designated as the head by resolution or by-law of a local public body (FIPPA s. 80)

## Access and Privacy Officer

- employee to whom the head has delegated a duty or power under section 81 of FIPPA (s. 1 of the Regulation)

## Access and Privacy Coordinator

- employee appointed to be responsible for receiving applications for access and for the day-to-day administration of FIPPA (s. 2 of the Regulation)



# RESPONSIBILITY FOR PRIVACY IN AN ORGANIZATION (PHIA)

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

## Head of a Public Body or Access and Privacy Officer

- if the trustee is also a public body, the Head of the public body or the delegated Access and Privacy Officer may make decisions or form opinions under PHIA

## Privacy Officer under PHIA

- employee designated by a health care facility or health services agency to deal with access requests and facilitate privacy compliance (PHIA s. 57)



# PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

**Record** means a record of information in any form, including paper records (correspondence, memos, notes), computer documents, email, photographs, films, video and sound recording

**Personal information** means recorded information about an identifiable individual, including the individual's name, age, ancestry, home address, home telephone number

**Personal health information** means recorded information about an identifiable individual that relates to

- the individual's health, or health care history, including genetic information
- the provision of health care to the individual
- payment for health care provided to the individual
- the Personal Health Identification Number (PHIN) and any other identifying number, symbol or particular assigned to an individual
- any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care



# PRIVACY UNDER FIPPA AND PHIA

M  
A  
N  
I  
T  
O  
B  
A

O  
M  
B  
U  
D  
S  
M  
A  
N

- **Part 3, Protection of Privacy**, of FIPPA and PHIA sets out obligations of public bodies and trustees concerning personal and personal health information
- **Personal Health Information Regulation** under PHIA also contains privacy requirements



# COLLECTION

There are three aspects of collection of personal or personal health information that must be considered:

- **purpose of collection:** collect only for purposes described in the Act (for example, if it is necessary for a function, activity or program)
- **limit on amount of information collected:** collect only as much as is reasonably necessary to accomplish the purpose for which it is collected
- **manner of collection/source of information:** collect directly from the individual unless one of the circumstances described in the Act applies to permit collection from another source



# NOTICE

If the personal or personal health information is collected directly from the individual, the public body/trustee must give notice of its collection practices and inform the individual of:

- the purpose for which the information is being collected
- the legal authority for the collection (FIPPA only)
- contact information of an employee who can answer the individual's questions about the collection

(FIPPA s. 37; PHIA s. 15)



# GENERAL DUTIES: USE AND DISCLOSURE

FIPPA and PHIA set out general duties of public bodies/trustees for use and disclosure of personal or personal health information:

- public body/trustee shall not use or disclose unless authorized under Act
- every use and disclosure must be limited to minimum amount necessary
- limit the use and disclosure to those employees or agents who need to know the information  
(FIPPA s. 42; PHIA s. 20)



# USE

A public body/trustee may only use personal and personal health information for the purpose for which it was collected

It cannot be used for another purpose unless one of the circumstances described in FIPPA or PHIA permit the use (also referred to as a “secondary use”)

(FIPPA s. 43; PHIA s. 21)



# DISCLOSURE

Personal and personal health information may only be disclosed by a public body/trustee if it is for a purpose described in the Act

(FIPPA s. 44; PHIA s. 22 and 23)



# SCENARIO 1: CASE DISCUSSION

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N



# SECURITY SAFEGUARDS

## Include:

- **Physical measures** such as locked drawers, rooms, offices and alarm systems
- **Technical measures** such as computer passwords, user verification, tracking systems
- **Administrative measures** such as written policies and procedures and employee education



# FIPPA: PROTECTION OF PERSONAL INFORMATION

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

- A public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, use, disclosure or destruction (FIPPA s. 41)
- PHIA has more developed safeguarding provisions than FIPPA and these must be the standard where the public body also maintains personal health information as a trustee under PHIA; for other public bodies, the PHIA standards would be a best practice



# PHIA: SECURITY SAFEGUARDS

A trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information (PHIA s. 18(1))

PHIA sets out:

- a list of specific safeguards (PHIA s. 18(2))
- reference to additional safeguards under regulation where personal health information is maintained in electronic form (PHIA s. 18(3))
- that a trustee shall take into account the degree of sensitivity of the personal health information to be protected (PHIA s. 19)



# PHIA REGULATION: SECURITY

PHIA Regulation 245/97 requires:

- a trustee to establish and comply with a written policy and procedures containing specific safeguarding provisions (PHIA s. 2)
- access restrictions within the organization, reasonable precautions to protect personal health information and secure storage (PHIA s. 3)
- additional safeguards for electronic health information systems (PHIA s. 4)
- authorized access for employees and agents (PHIA s. 5), orientation, training of employees about the written policy and procedures (PHIA s. 6), a pledge of confidentiality for employees and agents (PHIA s. 7)
- a security safeguard audit at least every two years (PHIA s. 8)



# RETENTION AND DESTRUCTION OF INFORMATION UNDER FIPPA

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

A public body that uses personal information about an individual shall - in the absence of another legal requirement - establish and comply with a written policy concerning the retention of personal information and the personal information must be retained for a reasonable period of time (FIPPA s. 40)

Public bodies that are departments of the Province of Manitoba are subject to *The Archives and Recordkeeping Act*



# RETENTION AND DESTRUCTION OF INFORMATION UNDER PHIA

A trustee shall:

- establish a written policy concerning the retention and destruction of personal health information and comply with that policy
- ensure that personal health information is destroyed in a manner that protects the privacy of the individual the information is about
- shall keep a record of the individual whose personal health information is destroyed, the time period it relates to, the method of destruction and the person responsible for supervising the destruction

(FIPPA s. 42; PHIA s. 20)



# SCENARIO 2: CASE DISCUSSION

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N



# PRIVACY BREACHES SEEN BY OMBUDSMAN

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

- Inappropriate disclosure of personal information without authorization
- Theft of laptop or files containing personal and personal health information from employee vehicles
- No written security policies and procedures or pledge of confidentiality as required by PHIA



# PRIVACY COMPLAINTS

An individual who believes that a public body or trustee has:

- collected
- used
- disclosed
- failed to protect in a secure manner (PHIA)

his or her own personal or personal health information contrary to the Act, may make a complaint to the Ombudsman

The Ombudsman may initiate complaints if satisfied there are reasonable grounds to investigate

(FIPPA s. 59; PHIA s. 39)



# DEALING WITH PRIVACY COMPLAINTS

- notify public body/trustee of the complaint
- informal process
- broad powers of investigation
- investigate in private
- right of complainant and public body/trustee to make representations
- written report of findings to complainant and public body/trustee
- power to make recommendations



# PRIVACY

- cannot be guaranteed despite safeguards used
- is only as strong as its weakest link
- will most likely be breached by an "insider", inadvertently or willfully
- if breached, is another example that "privacy lost cannot be regained"



# SOME BEST PRACTICES IN THE EVENT OF A PRIVACY BREACH

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

Immediately notify

- the FIPPA/PHIA personnel and other relevant personnel in the organization the police, if appropriate

Immediately start developing an action plan, including:

- attempting to mitigate the breach (for example, seek lost records)
- seeking help from the public through the media, if necessary (lost records)
- reviewing and, if necessary, revising policy and procedures advising staff in the organization of the breach and any remedial action and policy changes
- advising staff in the organization of the breach and any remedial action and policy changes
- using this as an educational opportunity within the organization



# SOME BEST PRACTICES IN THE EVENT OF A PRIVACY BREACH...CONT'D

As soon as possible after the breach:

- notify the person(s) whose privacy was breached of the event
- offer a meaningful apology
- advise that action plan is being undertaken

Also, as soon as possible after breach notify:

- Manitoba Ombudsman
- insurer, if appropriate
- lawyer, if appropriate

When all steps of the action plan are completed, or substantially completed:

- notify again the person(s) whose privacy was breached of actions taken
- notify again Manitoba Ombudsman of the actions taken



# MORE BEST PRACTICES

- Consent
- Privacy Impact Assessment
- Participants' Suggestions



# BUILDING PRIVACY AWARENESS IN YOUR ORGANIZATION

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

Understanding of privacy obligations under FIPPA and PHIA

Assess compliance with requirements

Well-informed employees are best defense against privacy breaches

Education and training of employees (ongoing, periodic sessions on privacy issues, posting privacy tips for employees, newsletter articles on privacy issues)



# RESOURCES

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N

## **Manitoba Health (PHIA)**

- PHIA website: [www.gov.mb.ca/health/phia/index.html](http://www.gov.mb.ca/health/phia/index.html)

## **Manitoba Culture, Heritage and Tourism (FIPPA)**

- [www.gov.mb.ca/chc/fippa](http://www.gov.mb.ca/chc/fippa)

## **Statutory Publications (Copies of Acts)**

- [www.gov.mb.ca/chc/statpub/](http://www.gov.mb.ca/chc/statpub/)

## **Manitoba Ombudsman**

- [www.ombudsman.mb.ca](http://www.ombudsman.mb.ca)



# MANITOBA OMBUDSMAN

## **Winnipeg Office (Ombudsman Act, FIPPA and PHIA)**

750-500 Portage Avenue

Winnipeg, MB R3C 3X1

Phone: (204) 982-9130

Toll-free: 1-800-665-0531

Fax: (204) 942-7803

## **Brandon Office (Ombudsman Act)**

603-1011 Rosser Avenue

Brandon, MB R7A 0L5

Telephone: (204) 571-5151

Toll free: 1-888-543-8230

Fax: (204) 571-5157

Our website: [www.ombudsman.mb.ca](http://www.ombudsman.mb.ca)

M  
A  
N  
I  
T  
O  
B  
A  
  
O  
M  
B  
U  
D  
S  
M  
A  
N