Updated: June 2019

The Personal Health Information Act

Micheal Harding
Legislative & Policy Analyst
Legislative Unit, Population Health Division
Manitoba Health, Seniors and Active Living

Manitoba

Online Resources

MHSAL PHIA Webpage:
https://www.gov.mb.ca/health/phia/index.html

PHIA Brief Summaries and Trustees' Guides:
https://www.gov.mb.ca/health/phia/trustees.html

The Manitoba Ombudsman's PHIA Page:
https://www.ombudsman.mb.ca/info/phia.html

Privacy Toolkit for Health Professionals:
https://www.gov.mb.ca/health/phia/resources.html

Further Training Required by PHIA

Important Reminder...

This course does not satisfy the legal requirement of Section 6 of the Personal Health Information Regulation for your employer to provide you with training about your employer's specific PHIA security policies and procedures.

If you have not received such training, you should ask your employer about it.

Outline

1. The Purpose of PHIA
2. Definitions
3. Access
4. Privacy
   - Collection, Use & Disclosure of PHI
5. Security
6. Compliance

1. THE PURPOSE OF PHIA

What is *The Personal Health Information Act* (PHIA)?

The *Personal Health Information Act (PHIA)* is a privacy law that establishes rules that trustees of personal health information must follow when collecting, using, disclosing, maintaining and destroying personal health information. PHIA also sets out the rights of individuals regarding obtaining access to and exercising control of their personal health information.

Why is it needed?

- A recent opinion survey suggests that Canadian patients change their behaviour in seeking health care if they perceive a risk to their privacy.

Canada: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes

http://www.FairWarning.com

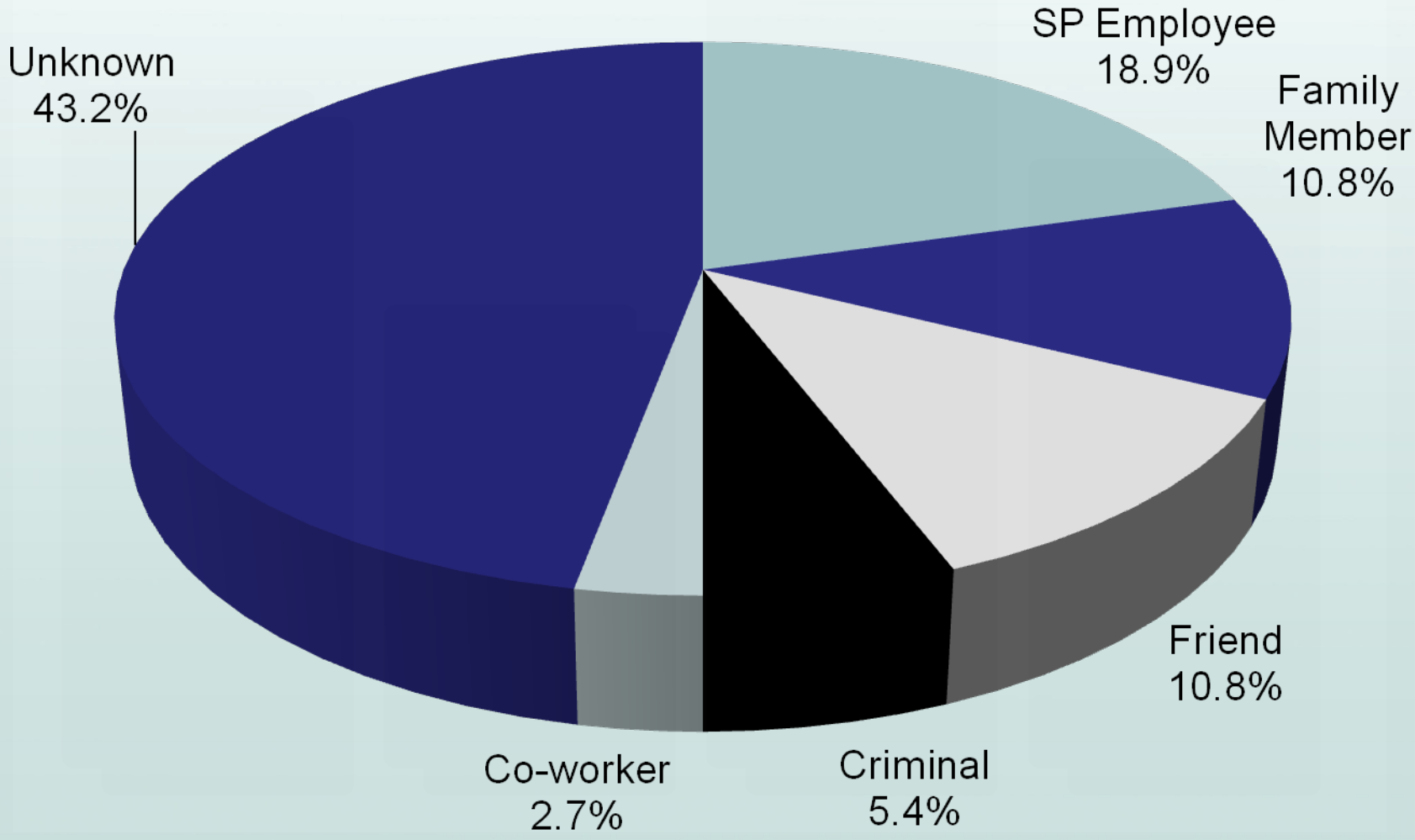
The survey methodology, results and conclusions are those of FairWarning.com. No official endorsement by Manitoba Health is intended or should be inferred.

Concerns over Privacy

- 61.9% reported that if there were serious or repeated breaches of patients' personal information at a hospital where they had treatment, it would reduce their confidence in the quality of healthcare offered by the hospital.
- 31.3% said they would postpone seeking care for a sensitive medical condition due to privacy concerns.
- 43.2% of the participants stated they would withhold information from their health care providers based on privacy concerns.
- 50.6% said they would choose to be treated at a different hospital.
- 42.9% said they would seek care outside of their community due to privacy concerns.

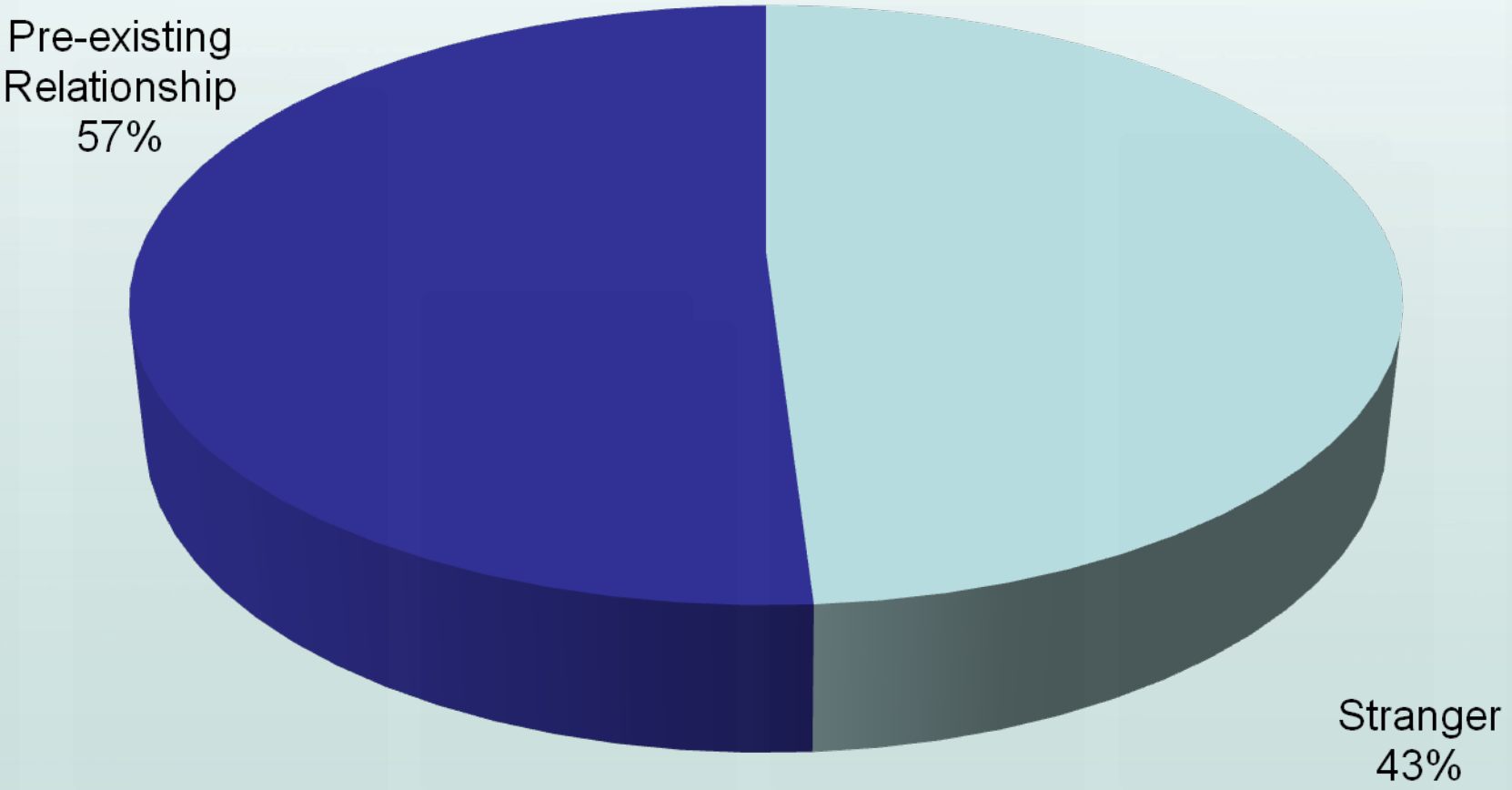
Manitoba

Breach Perpetrators



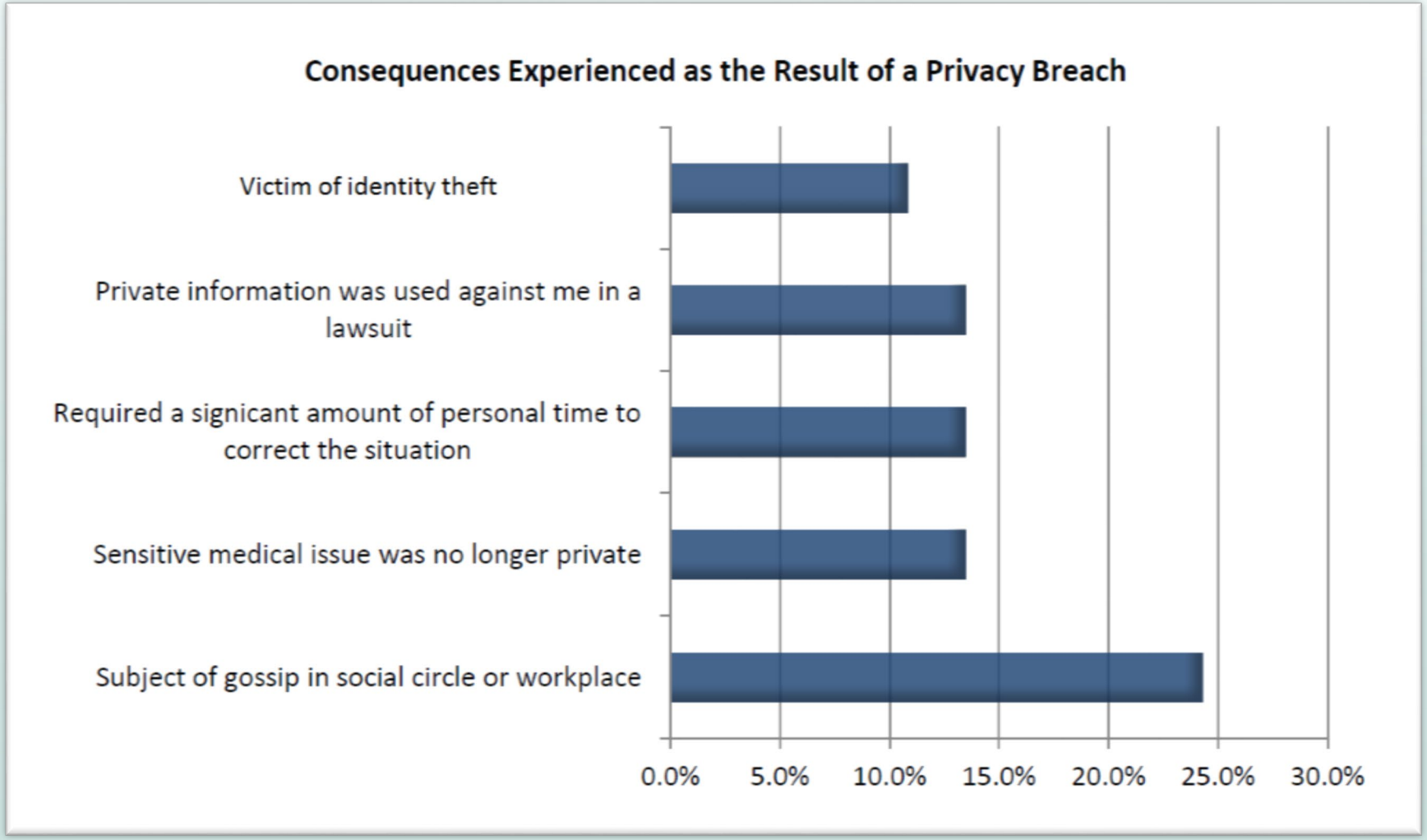
Manitoba

Breach Perpetrators



Manitoba

Figure 3: Canadian Patient Consequences Resulting from Privacy Breach



What does this mean?

Breaches of PHI

Reduced Confidence in Quality of Healthcare

Reduced Effectiveness of Healthcare

Fewer Positive Outcomes

Why is PHIA needed?

- Health information is personal and sensitive and its confidentiality must be protected so that individuals are not afraid to seek health care or to disclose sensitive information to health professionals;
- Individuals need access to their own health information as a matter of fairness, to enable them to make informed decisions about health care and to request the correction of inaccurate or incomplete information about themselves;
- A consistent approach to personal health information is necessary because many persons other than health professionals now obtain, use and disclose personal health information in different contexts and for different purposes;

2. DEFINITIONS

Trustees

- PHIA regulates the information practices of health information **trustees** defined as:
  - Licensed, Registered or Designated Health Professionals
  - Health Care Facilities
  - Health Services Agencies, and
  - Public Bodies (that collect and maintain personal health information)

Trustees

Definition continued

Subsection 61(2) of PHIA states that "Any action done by, or information disclosed to, a person employed by or in the service of a trustee in the performance of that person's duties is deemed to have been done by, or disclosed to, the trustee for the purposes of this Act."

Employees and agents of trustees are bound by PHIA.

Personal Health Information (PHI)

- **Personal Health Information (PHI)** means recorded information in any form about an identifiable individual that relates to:
  a) the individual's health, or health care history, including genetic information about the individual,
  b) the provision of health care to the individual, or
  c) payment for health care provided to the individual,

  and includes
  d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and
  e) any identifying information (I.E. demographic) about an individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care.

Representatives

- The following **representatives** can exercise another person's rights under PHIA (access and consent):
  - Anyone with written authorization from the individual;
  - A proxy under The Health Care Directives Act;
  - A committee under The Mental Health Act;
  - A substitute decision maker under The Vulnerable Persons Living with a Mental Disability Act;
  - If the individual is deceased, the executor or administrator of the estate; and
  - A parent or guardian of a minor who does not have the capacity to make their own health care decisions.

Representatives

- Where no such representative exists or is available, a family member or close friend may exercise the rights of an **incapacitated** person (Subsection 60(2)):
  a) the individual's spouse, or common-law partner, with whom the individual is cohabiting;
  b) a son or daughter;
  c) a parent, if the individual is an adult;
  d) a brother or sister;
  e) a person with whom the individual is known to have a close personal relationship;
  f) a grandparent;
  g) a grandchild;
  h) an aunt or uncle;
  i) a nephew or niece.

Privacy Breach

What is a breach?

- A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information or personal health information.
- Such activity is “unauthorized” if it occurs in contravention of applicable privacy legislation, such FIPPA and PHIA.
- Some of the most common privacy breaches happen when personal information is stolen, lost or mistakenly disclosed. A privacy breach may also be a consequence of faulty business procedure or operational breakdown.

3. ACCESS

Obligations of Trustees

- PHIA imposes two broad obligations on trustees:
  1. The obligation to grant individuals **access** to their own recorded personal health information, and
  2. The obligation to protect the **privacy** of personal health information.

Access

- Every individual has a right to access his or her own personal health information. This includes the right to:
  - Examine their PHI
  - Obtain a copy of their PHI, and
  - Request a correction to their PHI

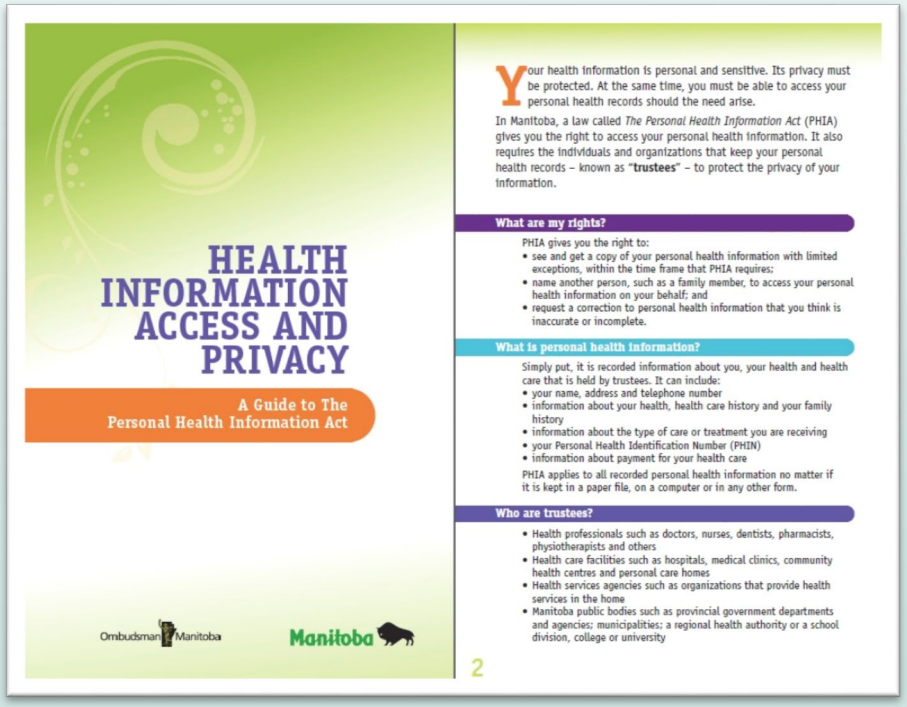
Notice of Right to Access

- Trustees must take reasonable steps to inform individuals of:
  - Their right to examine and receive a copy of their PHI;
  - How to exercise that right;
  - Their right to name a person to exercise their PHIA rights on their behalf.

Notice of Right to Access

Section 1.4 of the Personal Health Information Regulation

- For the purpose of section 9.1 of the Act, a trustee must use a sign, poster, brochure or other similar type of notice to inform individuals.
- The notice must be prominently displayed in as many locations and in such numbers as the trustee reasonably considers adequate to ensure that the information is likely to come to the individuals' attention.
- The notice may also contain other information about the trustee's practices and procedures relating to PHI, including information about the trustee's collection practices



HEALTH INFORMATION ACCESS AND PRIVACY

A Guide to The Personal Health Information Act

Ombudsman Manitoba

Manitoba

Your health information is personal and sensitive. Its privacy must be protected. At the same time, you must be able to access your personal health records should the need arise.

In Manitoba, a law called *The Personal Health Information Act* (PHIA) gives you the right to access your personal health information. It also requires the individuals and organizations that keep your personal health records – known as "**trustees**" – to protect the privacy of your information.

What are my rights?

PHIA gives you the right to:

- see and get a copy of your personal health information with limited exceptions, within the time frame that PHIA requires;
- name another person, such as a family member, to access your personal health information on your behalf; and
- request a correction to personal health information that you think is inaccurate or incomplete.

What is personal health information?

Simply put, it is recorded information about you, your health and health care that is held by trustees. It can include:

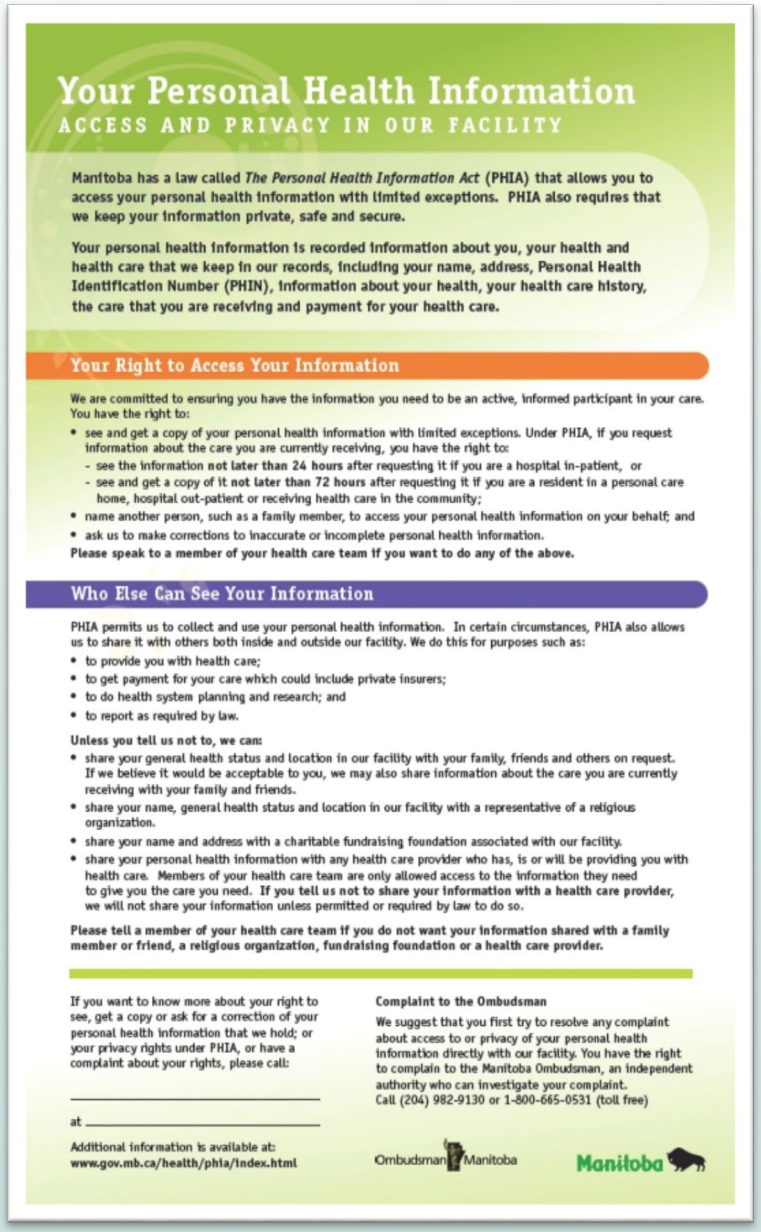
- your name, address and telephone number
- information about your health, health care history and your family history
- information about the type of care or treatment you are receiving
- your Personal Health Identification Number (PHIN)
- information about payment for your health care

PHIA applies to all recorded personal health information no matter if it is kept in a paper file, on a computer or in any other form.

Who are trustees?

- Health professionals such as doctors, nurses, dentists, pharmacists, physiotherapists and others
- Health care facilities such as hospitals, medical clinics, community health centres and personal care homes
- Health services agencies such as organizations that provide health services in the home
- Manitoba public bodies such as provincial government departments and agencies; municipalities; a regional health authority or a school division, college or university

2



Your Personal Health Information

ACCESS AND PRIVACY IN OUR FACILITY

Manitoba has a law called *The Personal Health Information Act* (PHIA) that allows you to access your personal health information with limited exceptions. PHIA also requires that we keep your information private, safe and secure.

Your personal health information is recorded information about you, your health and health care that we keep in our records, including your name, address, Personal Health Identification Number (PHIN), information about your health, your health care history, the care that you are receiving and payment for your health care.

Your Right to Access Your Information

We are committed to ensuring you have the information you need to be an active, informed participant in your care. You have the right to:

- see and get a copy of your personal health information with limited exceptions. Under PHIA, if you request information about the care you are currently receiving, you have the right to:
  - see the information **not later than 24 hours** after requesting it if you are a hospital in-patient, or
  - see and get a copy of it **not later than 72 hours** after requesting it if you are a resident in a personal care home, hospital out-patient or receiving health care in the community;
- name another person, such as a family member, to access your personal health information on your behalf; and
- ask us to make corrections to inaccurate or incomplete personal health information.

Please speak to a member of your health care team if you want to do any of the above.

Who Else Can See Your Information

PHIA permits us to collect and use your personal health information. In certain circumstances, PHIA also allows us to share it with others both inside and outside our facility. We do this for purposes such as:

- to provide you with health care;
- to get payment for your care which could include private insurers;
- to do health system planning and research; and
- to report as required by law.

Unless you tell us not to, we can:

- share your general health status and location in our facility with your family, friends and others on request. If we believe it would be acceptable to you, we may also share information about the care you are currently receiving with your family and friends.
- share your name, general health status and location in our facility with a representative of a religious organization.
- share your name and address with a charitable fundraising foundation associated with our facility.
- share your personal health information with any health care provider who has, is or will be providing you with health care. Members of your health care team are only allowed access to the information they need to give you the care you need. **If you tell us not to share your information with a health care provider, we will not share your information unless permitted or required by law to do so.**

Please tell a member of your health care team if you do not want your information shared with a family member or friend, a religious organization, fundraising foundation or a health care provider.

If you want to know more about your right to see, get a copy or ask for a correction of your personal health information that we hold; or your privacy rights under PHIA, or have a complaint about your rights, please call:

_____

at _____

Additional information is available at:
www.gov.mb.ca/health/phia/index.html

Complaint to the Ombudsman

We suggest that you first try to resolve any complaint about access to or privacy of your personal health information directly with our facility. You have the right to complain to the Manitoba Ombudsman, an independent authority who can investigate your complaint.
Call (204) 982-9130 or 1-800-665-0531 (toll free)

Ombudsman Manitoba

Manitoba

Access Requests

- Trustees' responsibilities:
  - To **assist** the person in making the request;
  - To **respond** to access requests within the time specified in PHIA; and
  - On request, to **explain** any term, code or abbreviation.

Timelines for Response

- Trustees must respond to access requests as promptly as required in the circumstances but not later than:
  - 24 hours if the individual is an in-patient in a hospital and the information is about *health care currently being provided* (for examination only);
  - 72 hours if the individual is not an in-patient in a hospital and the information is about *health care currently being provided;*
  - Within 30 days in any other case, unless the request is transferred to another trustee.

Refusing Access

- Access to personal health information can be denied as set out in subsection 11(1) of PHIA for the following reasons:
  a) Knowledge of the information could reasonably be expected to endanger the health or safety of the individual or another person;
  b) Disclosure of the information would reveal personal health information about another person who has not consented to the disclosure;
  c) Disclosure of the information could reasonably be expected to identify a third party who supplied the information in confidence;
  d) The information was compiled and is used solely peer review, review by a standards committee established to study or evaluate health care practice, quality or standards of professional services, or the purpose of risk management assessment; or
  e) The information was compiled principally in anticipation of, or for use in, a civil, criminal or quasi-judicial proceeding.

Severance of Information

- A trustee who refuses to permit personal health information to be examined or copied under Subsection 11(1) shall, to the extent possible, sever the personal health information that cannot be examined or copied and permit the individual to examine and receive a copy of the remainder of the information.

Privacy Officer

- Section 57 of PHIA requires a health care facility or health services agency to designate one or more of its employees as a privacy officer whose responsibilities would include:
  a) dealing with requests from individuals who wish to examine and copy or to correct personal health information under this Act; and
  b) generally facilitating the trustee's compliance with this Act (e.g. arranging training, tracking training)

4. PRIVACY

Privacy

- PHIA provides for privacy and confidentiality by imposing some restrictions on the:

  - ✓ **Collection,**
  - ✓ **Use,**
  - ✓ **Disclosure,**
  - ✓ **Retention,** and
  - ✓ **Destruction**

…of personal health information.

Privacy


SANTA'S GROTTO
CHRIS
BEFORE YOU TELL ME WHAT YOU WANT FOR CHRISTMAS I NEED YOUR FULL NAME, AGE, ADDRESS, PARENTS' OCCUPATIONS, THEIR INCOME, ASSETS, THEN JUST TO MAKE SURE YOU'VE BEEN A GOOD BOY - A SMALL TISSUE SAMPLE AND A LITTLE BOTTLE OF YOUR WEE-WEE.

Privacy - Collection

- A trustee has three main duties when **collecting** personal health information:
  1. Only collect as much information as is *necessary*;
  2. *Inform* the individual of the reason and purpose for which the information is being collected;
  3. Whenever possible, collect PHI *directly* from the individual the information is about:
     - It helps ensure the accuracy of the information;
     - It prevents trustees from revealing personal health information to others by the questions they pose;
     - It ensures that personal health information the individual wants to keep private is not revealed to the trustee.

Privacy - Use

- "*Use*" refers to the sharing of PHI internally.
- When *using* personal health information, trustees must:
  - Use personal health information for the *original purpose* it was collected (or for a purpose that is directly related);
  - Only use information for secondary purposes *with consent* or *where authorized* by section 21 of PHIA; and
  - Restrict use by *minimum amount* and *need to know* principles.

Permitted Uses w/o Consent

- Section 21 outlines purposes for which trustees can use PHI without prior consent:
  - Using an individual's demographic information or his or her Personal Health Identification Number (PHIN) to confirm eligibility for health care or payment for health care or to verify the accuracy of the demographic information or the PHIN;
  - Using an individual's demographic information to collect a debt the individual owes to the trustee or to the government if the trustee is a department;
  - To deliver, monitor or evaluate a program that relates to the provision of health care or payment for health care by the trustee.

Test Your Knowledge

“Use of PHI”

Scenario 1

- An employee accesses the electronic record of a co-worker in their employer's database to confirm the co-worker's date of birth so that a card can be signed and sent by the staff.

A) Appropriate

B) Not appropriate

Scenario 2

- An employee accesses their own personal health information in their employer's database.

A) Appropriate

B) Not appropriate

Scenario 3

- An employee of a trustee shares detailed, identifiable PHI with a co-worker to obtain his/her opinion related to the service being provided by the employee to the individual the information is about.

A) Appropriate

B) Not appropriate

Privacy - Disclosure

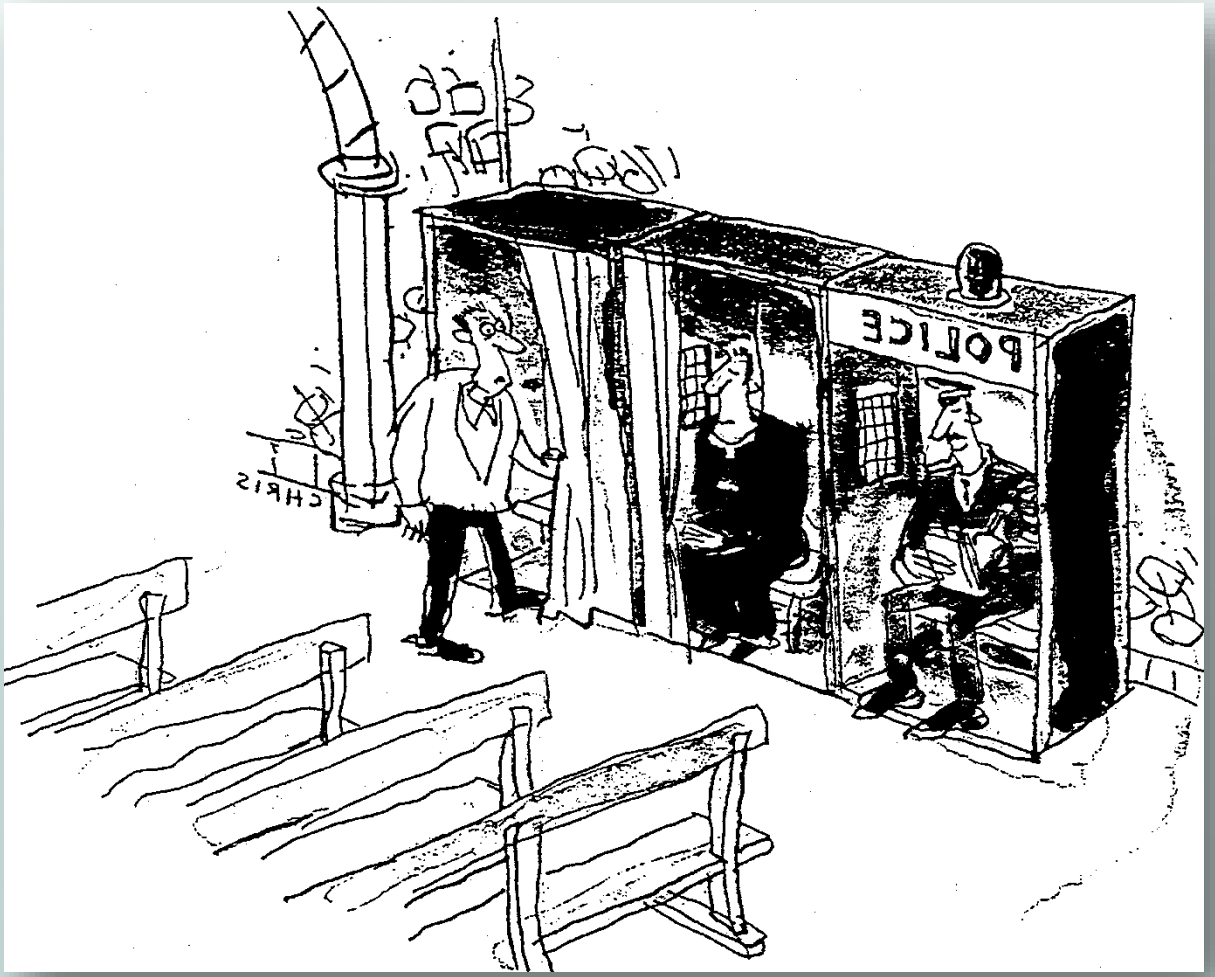
- "*Disclosure*" refers to sharing PHI with parties outside of your own organization.
- When *disclosing* personal health information, trustees must ensure that *authorization* for the disclosure exists.
- Authorization can be provided:
  - Through *consent* from the individual; or
  - Without consent where permitted by the Act.

Consent for Disclosure

- Must:
  - Relate to the purpose for which the information is used or disclosed
  - Be knowledgeable
  - Be voluntary
  - Not be obtained through misrepresentation
  - Be provided by the individual or his/her representative as defined in Section 60(1) and 60(2)

May be express or implied, except in specified Circumstances. Express consent need not be in writing.

Disclosure Without Consent



Disclosure Without Consent

- Section 22 of PHIA outlines the situations in which disclosure without consent is permitted. They include, but are not limited, disclosing:
  - To a person who is or will be providing or has provided health care to the individual, to the extent necessary to provide health care to the individual, unless the individual as specifically said not to;
  - To prevent or lessen a serious and immediate threat to the health or safety of the individual the information is about or another individual, or public health or public safety;
  - To prevent or lessen a risk of harm to the health or safety of a minor;
  - To a person for the purpose of contacting a relative or friend of an individual who is ill, injured, incapacitated or deceased;
  - For the purpose of peer review by health professionals, or to study or evaluate health care practices or the quality or standards of professional services;
  - For the purpose of delivering, evaluating or monitoring a program of the trustee;
  - For an investigation respecting 1) payment for health care, or 2) a fraud relating to payment for health care; and
  - When authorized or required by an enactment of Manitoba or Canada (I.E. CFSA, MPA, VPA, PPCA).

Duty to Report

- Subsections 18(1) and 18(1.1) of *The Child and Family Services Act* (CFSA) requires a person who has information that leads the person reasonably to believe that a child is or might be in need of protection is required to report the information to an agency or to a parent or guardian of the child. The person must report directly to an agency if they reasonably believe that the parent or guardian
    I. is responsible for causing the child to be in need of protection, or
    II. is unable or unwilling to provide adequate protection to the child in the circumstances;

- Subsection 21(1) of *The Vulnerable Persons Living with a Mental Disability Act* (VPA) requires any person who believes on reasonable grounds that a vulnerable person is, or is likely to be abused or neglected, immediately report that belief.

- Subsection 3(1) of *The Protection for Persons in Care Act* (PPCA) requires any service provider or other person who has a reasonable basis to believe that a patient is, or is likely to be, abused to promptly report the belief, and the information on which it is based.

Disclosures

- Employees should only disclose PHI where the disclosure is consistent with the employee's defined role and function. Directors/managers will determine which employees are authorized to make disclosures.
- Where a request for disclosure is received from a third party organization, these requests are encouraged to be in writing.
- Records of disclosures, including reasons and authority should be maintained.
- Disclosure for research is only done with approval of an institutional research review committee.

Retention & Destruction

- Retention & Destruction of PHI must be in accordance with established policies and procedures.
- When destroying PHI, it must destroyed in a manner that preserves the confidentiality of the information.
  - Personal health information of any sort must never be discarded in mainstream garbage.
  - CDs and other similar storage media should be physically destroyed.
  - PHI held on a computer or in the memory found in other electronic equipment, such as photocopiers and fax machines, needs to be magnetically erased or overwritten in such a way that the information cannot be recovered.

Your workplace should have policies and procedures in place for the secure disposal of PHI.

Test Your Knowledge

“Disclosure of PHI”

Scenario 1

- A physician at St. Boniface Hospital shares detailed, identifiable PHI with a colleague who works at Brandon Regional Health Centre to obtain his/her opinion related to the service being provided by the physician to the individual the PHI is about.

  A) Appropriate

  B) Not appropriate

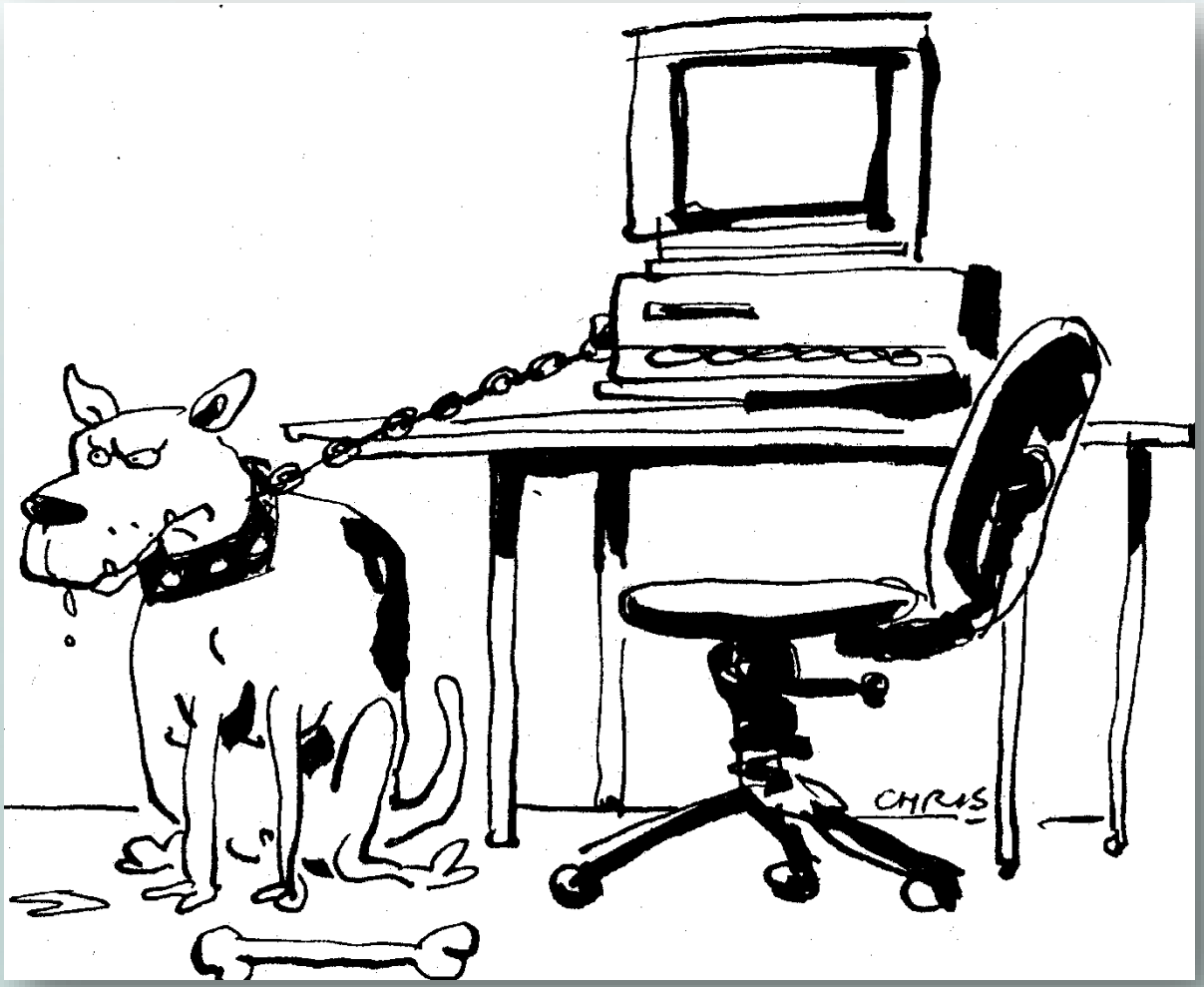
Scenario 2

- The RCMP calls, informing you that they are conducting a missing person investigation, and that they require the date and reason for the recent visit of a patient. This disclosure is…
    A. authorized
    B. not authorized

Scenario 3

- An email is received from an individual, stating that they are a CFS worker conducting a child protection investigation and that they require the address a child that must be urgently apprehended. You…
    A. disclose the information, or
    B. tell them you cannot disclose the information.

5. Security


CHRIS

Security

PHIA requires trustees to protect the confidentiality, security, accuracy and integrity of PHI by adopting reasonable safeguards, which may include:

1. Physical safeguards
   - E.G. proximity reader ID badges, locked rooms and sections, lockable filing cabinets
2. Technical safeguards
   - E.G. passwords, secure networks, encryption software, firewalls, antivirus
3. Administrative safeguards
   - E.G. policies, procedures, training, pledges

Safeguards must be appropriate to the sensitivity of the information.

Required Policies

A Trustee is required to establish a written policy/procedure containing:

- provisions for the security of PHI during its collection, use, disclosure, storage, and destruction. These provisions must include measures to ensure the security of PHI:
  - when a record of the information is removed from a secure designated area
  - in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose
- provisions for the recording of security breaches
- corrective procedures to address security breaches
- provisions regarding the retention and destruction of PHI

Record of User Activity

- The Personal Health Information Regulation requires trustees to maintain a record of user activity for any electronic information system it uses to maintain PHI, which identifies the following:
  a) individuals whose PHI has been accessed,
  b) persons who accessed PHI,
  c) when PHI was accessed,
  d) the electronic information system or component of the system in which PHI was accessed,
  e) whether PHI that has been accessed is subsequently disclosed under section 22 of the Act;

<u>Trustees will provide this record upon request.</u>

Auditing

- Subsection 4(4) of the Personal Health Information Regulation requires trustees to audit records of user activity to detect security breaches. Audits could be conducted on any or all of the following triggers:
  - attempts to access information based on same family name, address or user name, human resource related events, or high profile name;
  - abnormal number or frequency of login attempts; and
  - high volume of activity associated with a single subject of care.

PHIA Training

- Subsection 6 of the Personal Health Information Regulation requires trustees to provide orientation and ongoing training for its employees and agents about the trustee's PHIA security policies and procedures.

MHSAL PHIA Online Training Program

http://www.trainingtodo.com/mbhealth/secure/index.asp

Pledge of Confidentiality

- All employees, students, volunteers, non-paid staff and individuals providing professional services to a trustee under contract should be required to sign a Pledge of Confidentiality.
- Must include an acknowledgment that he or she is bound by any PHIA Policies & Procedures of the trustee.
- Employees must be informed of the consequences of breaching those policies and procedures.

PHIA Pledge of Confidentiality (sample)

Other advisable policies…

- Passwords
- Transmitting PHI
- Working with PHI
- Portable PHI
- Approved Devices
- Social Media

6. Compliance

Complaint Process

- An individual has a right to make a complaint to the Manitoba Ombudsman regarding any practice under PHIA or FIPPA.

- A Compliance Review can be initiated by a complaint when an individual believes a trustee is in breach of its obligations under PHIA.

Information and Privacy Adjudicator

- Appointed under *The Freedom of Information and Protection of Privacy Act.*
- Enables the Ombudsman to refer matters for compliance review.
- Adjudicator is able to make binding access and privacy orders, which may be subject to judicial review.

Penalties for Violations

- The Act provides for a fine of up to $50,000 for a violation of the Act. This fine can be imposed for each day that an offence continues.

To what offences will this penalty apply?

  - Deliberately erasing or destroying PHI to prevent an individual from getting access to it;
  - Collecting, using, selling or disclosing PHI in violation of the Act; and
  - Failing to protect PHI in a secure manner.

Penalties for Violations

- **To whom will the penalty apply?**
  - Trustee organizations (corporations)
  - Directors or Officers
  - Employees of a trustee for:
    - Deliberately erasing PHI
    - Deliberately destroying PHI
    - Wilfully disclosing PHI
    - Obtaining PHI through misrepresentation
    - Using, gaining access to or attempting to gain access to PHI without authorization
    - Knowingly falsifying PHI

Final Thoughts…

- Every employee must ensure that the information they use in the course of their duties

  a) is done so in accordance with PHIA

  b) is maintained in a safe and secure manner.

For more information, contact:

Legislative Unit, Health Population Division
Manitoba Health, Seniors and Active Living
Tel: (204) 788-6612
Email: PHIAinfo@gov.mb.ca