The Personal Health Information Act (PHIA)

. . . . . .

Manitoba Health

Manitoba

Purpose

1. To provide you with an introduction to *The Personal Health Information Act (PHIA)*
2. To provide you with a overview of the requirements within the Regulations
3. To help you to understand the principles
4. To help you comply with the requirements

Outline

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

1. THE PURPOSE OF PHIA

The Purpose of PHIA

- 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;

- 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

Survey Overview

- Commissioned in October 2011
- Live for 6 days
- 20,937 patients invited to participate online
- Sent to residents of all provinces in Canada including urban metropolitans and rural communities.
- 1002 individuals responded

Survey Purpose

- To measure how privacy considerations affect patient behaviours and decisions and influence patient care outcomes.

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.

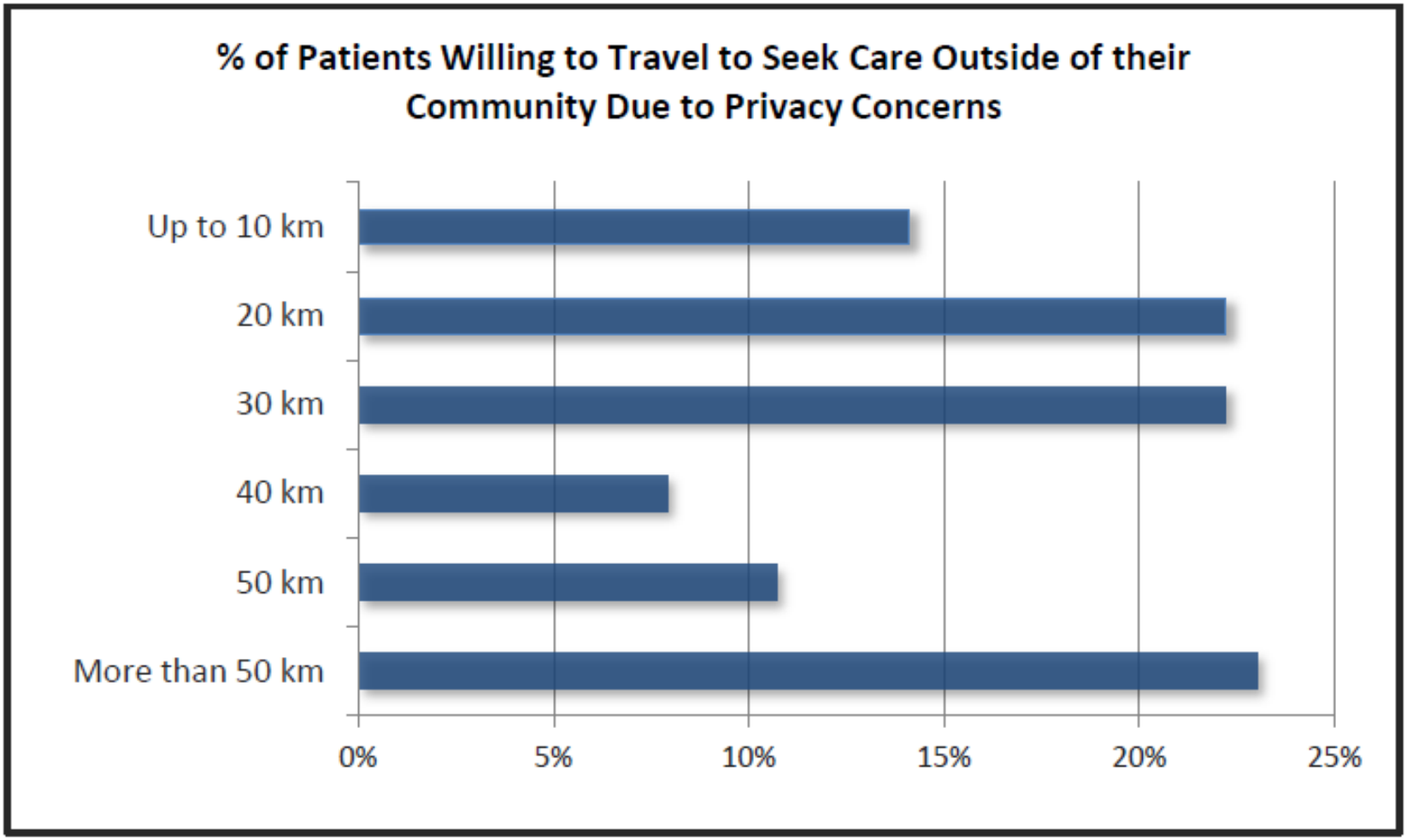
- 31.3% said they would postpone seeking care for a sensitive medical condition due to privacy concerns.

- 43.2% of the participants stated they would withhold information from their health care providers based on privacy concerns.

- 42.9% said they would seek care outside of their community due to privacy concerns.

Manitoba

Figure 1: Patients' Willingness to Travel to Avoid Privacy Concerns



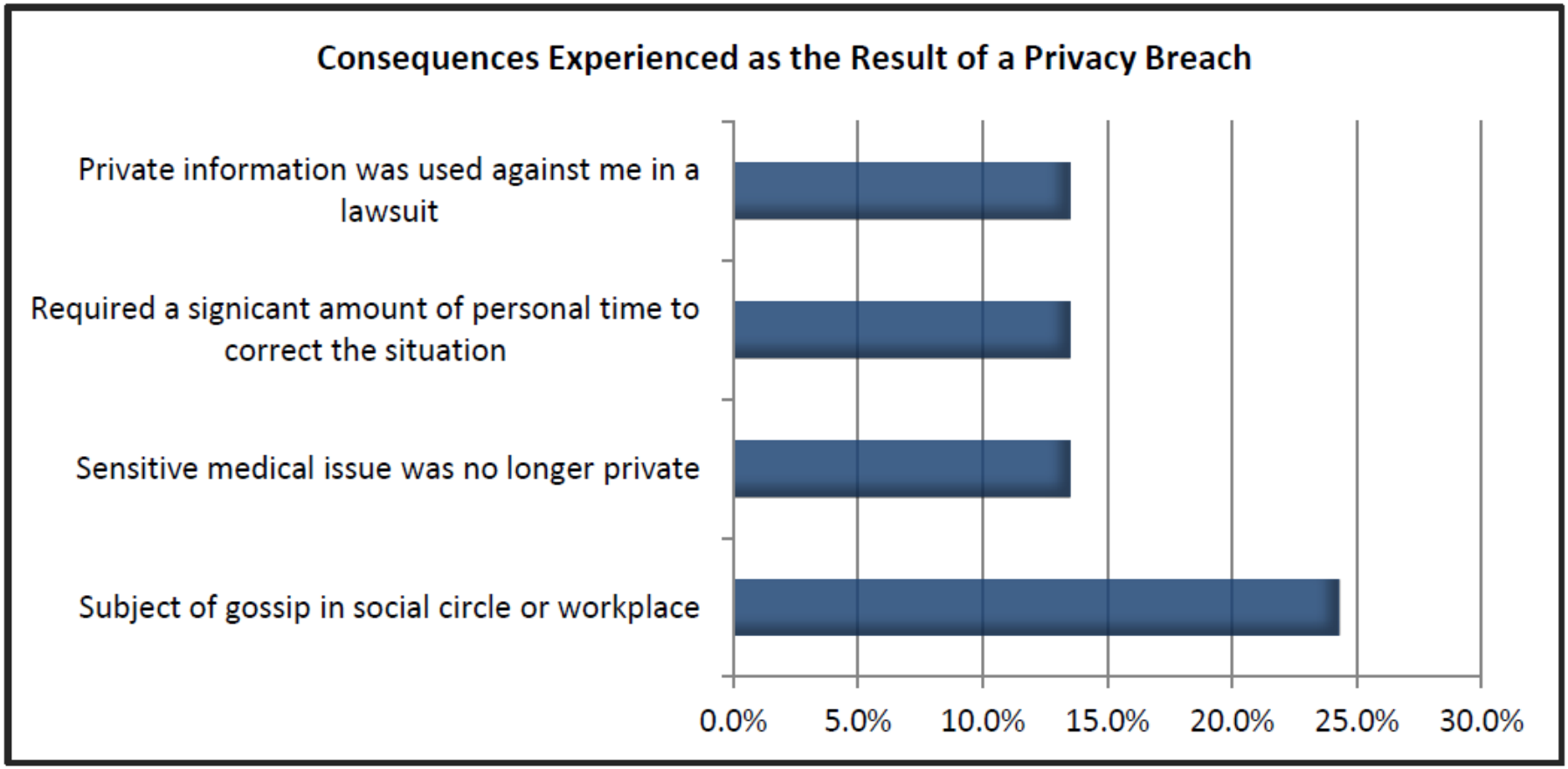
Breach Perpetrators

- 3.7% of Canadian patient respondents indicated they had been alerted or discovered on their own that their medical records had been compromised:
  - 18.9% were committed by an unknown employee of the hospital or healthcare provider where the patient sought care;
  - 10.8% were committed by a family member;
  - 10.8% were committed by a friend;
  - 5.4% were committed by a member of a crime ring or criminal; and
  - 2.7% were committed by a co-worker.

In 43.2% of cases the perpetrator is still unknown.

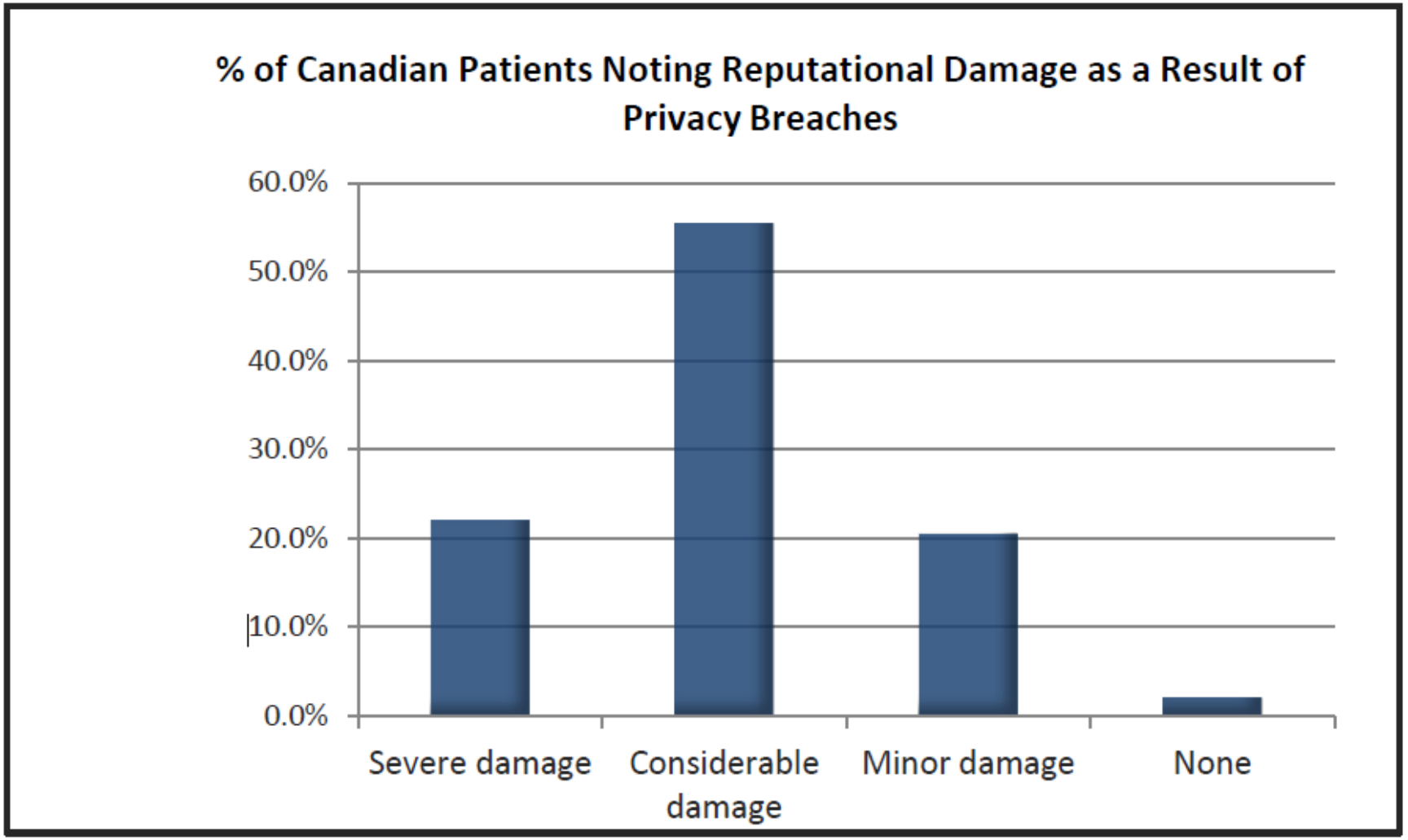
Manitoba

Figure 3: Canadian Patient Consequences Resulting from Privacy Breach



Manitoba

Figure 2: Patient Perception of Reputational Damage as a Result of Privacy Breaches



Survey Summary

- Because of privacy concerns, patients will:
  - Withhold information
  - Postpone seeking healthcare
  - Travel outside their community (86% 20 km or more)
- 76% report considerable or greater damage to their reputation as a result of breaches of PHI, with almost 1 in 4 feeling that they have become a subject of gossip, despite up to 50% of those breaches being perpetrated by someone well-known to them.

What does this mean?

Breaches of PHI

Reduced Confidence in Quality of Healthcare

Reduced Effectiveness of Healthcare

Fewer Positive Outcomes

2. DEFINITIONS IN THE ACT

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)

Employees and agents of trustees are bound by PHIA.

Personal Health Information

- PHIA governs the collection, use, disclosure, retention and destruction of personal health information (PHI) that:
  - Is in any form;
  - Is about an identifiable (or potentially identifiable) individual;
  - Relates to an individual's health status, health history, health services received;
  - Includes any identifying numbers or symbols;
  - Includes demographic information (name, date of birth, phone number, address, e-mail address) collected in the course of, and 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
  - 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 (Section 60(1), 60(2), and 60(3)):
  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.

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.

3. ACCESS

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.

Posters and pamphlets are available from Manitoba Health for this purpose.

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 section 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.

Random Trivia

- A woman calls stating she is the wife of resident of Selkirk Mental Health Centre. She requests a billing list of doctors and mental health professionals her husband has seen in the last ten years. She can provide ID and proof of marriage. How do you respond and why?

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

- General Limitations:
  - **Less is best.** Trustees should only collect, use and disclose the **minimum amount** of information necessary for an identified purpose.
  - Trustee and employee access should be limited based on the **need to know** principle.
  - Privacy is not an absolute right. Other competing social interests are balanced in the law (e.g. serious and immediate dangers, public health threats, child abuse).
  - Emphasizes the importance of thinking twice before accessing or disclosing Personal Health Information.

Privacy - Collection

- A trustee has three main duties when **collecting** personal health information:
  1. *Inform* the individual of the reason and purpose for which the information is being collected;
  2. Only collect as much information as is *necessary***;**
  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.

Collection from Another Source

- Collect from another source other than the individual the information is about is permitted when:
  - the individual has authorized another method of collection;
  - collection could endanger the health or safety of the individual;
  - time or circumstances do not permit collection from the individual;
  - collection of the information directly from the individual could reasonably be expected to result in inaccurate information being collected;
  - the information is collected for the purpose of compiling a family/genetic history, determining/verifying the individual's eligibility for a program/benefit/service of 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 unrelated purposes *with consent* or *where authorized* by section 21 of PHIA; and
  - Restrict use by *minimum amount* and *need to know* principles.

Test Your Knowledge

- It is acceptable to look up the date of birth of a co-worker so that a card can be signed and sent by the staff.

  A) Yes

  B) No

  C) Only if the their exact age is not revealed.

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 permission need not be in writing.

Disclosure Without Consent

- Section 22(2) 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;**
  - **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 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. The Child and Family Services Act).**

Disclosure Without Consent

- *Unless the patient tells the facility not to*, a hospital/PCH may share information with:

1. A religious organization – name, general health status and location
2. A charitable fundraising organization – name and mailing address

Privacy - Retention

- The Canadian Medical Protective Association (CMPA) advises that medical records should be retained for 10 years from date of last entry or in case of minor, age of majority plus 10 years (as per By-law #1 under the *Medical Act*).

Privacy - Destruction

- When **destroying** personal health information, trustees must ensure that it is destroyed in a manner that **preserves the confidentiality** of the information.

Random Trivia

- The RCMP calls, informing you that they are conducting a missing person investigation, and that they require the date and reason for admission of an in-patient. You…
    A. give them the information;
    B. pass them to your supervisor;
    C. tell them you cannot release that information.

5. Security

Privacy - Security

- To ensure the *security* of personal health information, trustees must have:

    1. Physical safeguards
        - E.G. locked rooms, filing cabinets
    2. Technical safeguards
        - E.G. passwords, secure networks
    3. Administrative safeguards
        - E.G. policies, orientation, pledges

Safeguards must be appropriate to the sensitivity of the information.

Security

- Trustees are responsible for ensuring that:
  - PHI is only provided to authorized persons (internally and externally);
  - Identity & authority of individuals requesting PHI is correct;
  - Physical, technical, and administrative security safeguards are in place and are appropriate to the sensitivity of the information they maintain.
  - Reasonable precautions are taken to protect PHI from fire, theft, vandalism, deterioration, accidental destruction, loss, or any other hazards.

Individual Security

- Employees of trustees are responsible for:
  - Where applicable, ensuring all visitors are registered and issued visitor passes before being admitted to secure areas.
  - Challenging and, if necessary, reporting to security any unrecognized individual in secure areas or in areas where PHI is maintained or accessible.
  - Ensuring that PHI in both paper and electronic format is not left in open view when employees are away from their work areas.
  - When PHI is removed from the work site, the employee is responsible for protecting the information at all times from unauthorized access, use, disclosure, reproduction, alteration, loss, or destruction.

Insufficient Security

- Examples of insufficient security:
  - Paper records stored in an area accessible to the public;
  - Improperly stored passwords;
  - Emailing personal health information over an unprotected network (E.G. the internet) without encryption; and
  - Providing personal health information over the phone without verifying the identity of the individual.

Random Trivia

- Your supervisor tells you to provide your network ID and password so that a branch/unit list can be compiled and kept on hand in case of emergency. Do you say:

  A) Sure thing!

  B) No way!

  C) Has the director approved this?

Healthcare Related Breaches

- Mistakenly published PHI exposed in Newfoundland: File Sharing Software Exposes Records

- Risk Mitigation:
  - File sharing programs (I.E. Torrent) must not be downloaded onto workstation or notebook computers.
  - Be conscious of what programs access the internet and why they access it.

- 75,000 individual's health records lost on unencrypted CD: Subcontractor loses data in shipment

- Risk Mitigation:
  - Data on removable storage devices should ALWAYS be encrypted and passworded.

- Western Health Regional Health Authority in Newfoundland is facing a class action lawsuit after an employee was fired for inappropriately accessing the medical records of 1,043 patients.

- Risk Mitigation:
  - Do not share passwords for information systems.
  - Lock your terminal when you leave it.
  - Log out at the end of your shift.
  - Perform random audits.

- Laptop Stolen From Physician's Car: Toronto Hospital for Sick Kids Contacting Individuals Involved in 10 Different Studies

- Risk Mitigation:
  - PHI must never left unattended and in plain view of unauthorized persons.
  - If PHI must be left in a vehicle, it must be locked in a trunk or placed in a comparable secure area where it cannot be seen from outside the vehicle.
  - Information should be placed out of view before arriving at the location where the vehicle will be parked.
  - PHI must never be left in a vehicle parked in a high risk area (e.g. shopping mall parking lot) even if the information is stored out of view.

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;

6. Compliance

Compliance Review

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

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

Penalties for Violations

- To whom will the penalty apply?
  - Health Care Facilities
  - Directors or Officers
  - Employees of a trustee for:
    - Deliberately erasing PHI
    - Deliberately destroying PHI
    - Wilfully disclosing PHI
    - Obtains PHI through misrepresentation

7. Obligations

Pledge of Confidentiality

- All trustee employees, students, volunteers, non-paid staff and individuals providing professional services to the trustee under contract are required to sign a Pledge of Confidentiality.
- This pledge should include reference to any policies & procedures under PHIA of the trustee.
- Consequences should range from disciplinary action to termination of employment.

A Trustee's Guide to **The Pledge of Confidentiality**
Required by The Personal Health Information Act is available online.

Ethical Obligation

- As trustees, or employees of trustees, there is an ethical obligation to guard PHI.

- All employees of trustees are responsible for ensuring that the information they use in the course of their duties is maintained in a safe and secure manner.

Policy &Procedures

- What do you do if you become aware of a breach of PHI or a situation which could reasonably be expected to result in a breach?

Trustees are required in Section 2 of the Regulations to establish and comply with a written policy and procedures regarding the security of PHI, including provisions for corrective procedures to address security breaches. At minimum, you should:

1. immediately take any practicable steps to cease or lessen the breach, and
2. report the breach to a superior as soon as possible.

Guiding Principles

1. Ask questions
2. Minimum Necessary
3. Need to Know
4. When in doubt, ask.
5. Conduct yourself appropriately

Online Resources

Manitoba Health PHIA Website:
http://www.gov.mb.ca/health/phia/index.html

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

The Manitoba Ombudsman's PHIA Page:
http://www.ombudsman.mb.ca/phia.htm

For More Information…

Contact:

Legislative Unit
Manitoba Health
Tel: (204) 788-6612