DUTY TO NOTIFY INDIVIDUAL OF PRIVACY BREACH – [SECTION 19.0.1 of PHIA]

Summary: *Effective January 1, 2022, The Personal Health Information Act (PHIA) and the Personal Health Information Regulation will be amended to provide that a trustee who maintains personal health information about an individual must notify the individual about a privacy breach relating to the information if, after considering the relevant factors prescribed in the regulations, the breach could reasonably be expected to create a real risk of significant harm to the individual. Please note that determining whether or not an individual must be notified of a privacy breach does not impact the responsibility to investigate and implement measures to address a privacy breach and to prevent similar privacy breaches from occurring in the future*

What is a privacy breach?

Privacy breaches occur when personal health information is:

- stolen
- lost
- accessed
- used
- disclosed
- destroyed
- altered

in contravention of PHIA and its regulations.

What is an example of a privacy breach?

Examples of privacy breaches may include:

(i) the loss or theft of mobile devices (ex: laptops, USB sticks),
(ii) the theft of personal health information through computer hacking,
(iii) misdirected communication (ex: fax, email, mail),
(iv) employees of a trustee accessing, using or disclosing the information other than for the purposes of performing their job duties,
(v) personal health information being destroyed in a manner that is not secure, or
(vi) alteration of personal health information for purposes other than correcting errors in the information.

Do I have to report privacy breaches to someone? Do I need to report all breaches?

Trustees are required to notify the individual whose information was subject to the privacy breach as soon as practicable after the privacy breach becomes known to the trustee, where a privacy breach could reasonably be expected to create a real risk of significant harm to the individual.

Whether a privacy breach affects one person or a 1,000, it will still need to be reported if the trustee's assessment indicates there is **a real risk of significant harm** resulting from the breach.

What is real risk of significant harm?
"Significant harm" includes, in relation to an individual, bodily harm, humiliation, damage to the individual's reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the individual's credit rating or report, and damage to or loss of the individual's property.

Section 8.7 of the Personal Health Information Regulation sets out the list of factors that trustees must consider in determining if a privacy breach could reasonably be expected to create **a real risk of significant harm** to an individual, including:

(a) the **sensitivity** of the personal health information involved;
(b) the **probability** that the personal health information could be used to cause significant harm to the individual;
(c) any other factors that are reasonably relevant in the circumstances.

As a part of their assessment, trustees should consider the following:

A) Sensitivity:
PHIA and its regulations do not define the term "sensitivity". However, the concept of sensitivity of personal health information is discussed in PHIA's Preamble, which states:

*"… 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."*

To determine the sensitivity of the personal health information, it is important to examine both what personal health information has been involved in the breach and the circumstances surrounding the breach.

While all health information is generally considered to be sensitive, certain health information is considered more sensitive because of the specific risks to individuals when said information is stolen, lost, accessed, used, disclosed, destroyed or altered in contravention of PHIA, including information that could be used for identity theft or fraud. For instance, an individual's Personal Health Identification Number (PHIN) is considered highly sensitive and is subject to additional protections in PHIA.

Other personal health information, for instance a patient or client file, a medical diagnosis, psychological or counselling information, list of medications, emergency contacts, or other information, may have varying degrees of impact on the individual.

Certain information may on its face be clearly sensitive. Other information may not be. The circumstances of the breach may make the information more or less sensitive. The potential harms that could accrue to an individual are also an important factor.

B) Probability

Subsection 8.7(b) of the Personal Health Information Regulation sets out the factors to be considered by a trustee to determine the probability that the personal health information subject to the breach could be used to cause significant harm to the individual are:

(i) the event that caused the privacy breach to occur, including whether there is evidence of any malicious intent, such as the breach being the result of theft or gaining unauthorized access to a computer system,
(ii) the number of persons who actually or potentially accessed the personal health information,
(iii) if the identity of the persons who actually or potentially accessed the personal health information is known or unknown,
(iv) any known relationship between any of the persons who actually or potentially accessed the personal health information and the individual to whom the information relates, and the nature of the relationship,
(v) if the trustee is reasonably satisfied that any person who actually or potentially accessed the personal health information has destroyed any unauthorized copies of it and has committed to not use or disclose it,
(vi) the length of time since the privacy breach first occurred and the duration of the period in which the personal health information was available to be accessed, used, disclosed, destroyed or altered in contravention of the Act,
(vii) the amount of personal health information involved,
(viii) if the personal health information has been recovered,
(ix) if the personal health information was adequately encrypted, anonymized or otherwise not easily accessible, and
(x) if harm has materialized.

Notice to the individual must be given as soon as practicable after the privacy breach becomes known to the trustee, and subsection 8.8(1) of the Personal Health Information Regulation provides that it must be given in writing and must include:

a) a description of the circumstances of the privacy breach;
b) the date or period of time that the privacy breach occurred, or is believed to have occurred;
c) the name of the trustee who had custody or control of the personal health information at the time of the privacy breach;
d) a description of the personal health information that was the subject of the privacy breach;
e) a description of the steps that the trustee has taken or is intending to take, as of the date of the notice,
    (i) to reduce the risk of harm to the individual as a result of the privacy breach, and
    (ii) to reduce the risk of a similar privacy breach in the future;
f) a description of the steps that the individual can take to reduce the risk of harm that can result from the privacy breach or to mitigate that harm;
g) a statement that the Ombudsman has been, or will be notified about the privacy breach, as required under subsection 19.0.1(4) of the Act;
h) the name and contact information of an officer or employee of the trustee who is able to answer questions about the privacy breach; and
i) any other information that the trustee considers relevant.

C) Any Other Factors That Are Reasonably Relevant In The Circumstances

The Personal Health Information Regulation is silent on what other factors are reasonably relevant in the circumstances.

What is direct notification?

Direct notification is when a trustee notifies an individual by communicating with them in writing or orally.

Subsection 8.8(2) of the Personal Health Information Regulation provides that notice may be given orally only if the trustee reasonably believes that the delay necessary to provide written notice to an individual is likely to significantly increase a real risk of significant harm to the individual. If notice is given orally, the trustee must record the information that was given and the date on which it was provided, or the trustee must give the individual notice in writing within a reasonable time after the oral notice is provided.

When can I indirectly notify individuals?

There are limited times when a trustee can indirectly notify people, meaning there is no direct written or oral communication with the individual.

Subsection 8.8.1(1) of the Personal Health Information Regulation provides that indirect notification may be given when:

- the trustee reasonably believes that the privacy breach may result in a risk to public health or safety;
- if the identity or current contact information of the individual or individuals is not known; or
- if the trustee reasonably believes giving written notice is impractical or unduly expensive because of the large number of individuals that may have been affected by the privacy breach, or because it could threaten or harm the individual's mental or physical health.

What are examples of indirect notification?

Subsection 8.8.1(2) of the Personal Health Information Regulation provides that indirect notification must be given by:

- **public communication or similar measure** that
  i) can be reasonably expected to reach the affected individual or individuals, and
  ii) does not include any information that could reasonably identify the affected individual or individuals; or
- **in writing to an individual who provides care to the recipient or to an individual with whom the recipient is known to have a close personal relationship,** if notice of the privacy breach can be reasonably expected to threaten or harm the recipient's mental or physical health.

Trustees must use a public communication or similar measure that can be reasonably expected to reach the affected individual or individuals. For example, mentioning the privacy breach in a corporate blog post may not have the same expected reach that a prominent and dedicated public announcement campaign would have. Trustees should consider all potential options available for use in future public communications. For example, trustees may consider how to incorporate media messaging, including for instance a prominent notice made on its website or other online/digital presence.

In addition, where a trustee provides notice of a privacy breach to an individual under section 19.0.1 of PHIA, the trustee is required to report privacy breaches to the Office of Manitoba Ombudsman. A form for reporting a privacy breach to the Office of the Manitoba Ombudsman has been posted on the Ombudsman's website, and is available for anyone to use.

Can I add new information to a report already sent?

Yes. If trustees become aware of any new information, they may report that information.

Do I have to maintain an internal record of privacy breaches?
Trustees are required to take steps that are reasonable in the circumstances to ensure that the personal health information in their custody or control is protected appropriately. As a best practice, maintaining an internal record of all privacy breaches that occur is recommended. A trustee may consider implementing a record that includes:

- date or estimated date of the breach;
- general description of the circumstances of the breach;
- description of information involved in the breach; and
- whether or not the breach was reported to the Manitoba Ombudsman/individuals were notified;
- a description of the steps that the trustee has taken or is intending to take to reduce the risk of harm to individuals as a result of the privacy breach, and to reduce the risk of a similar privacy breach in the future;
- any other details that the trustee considers relevant.

The record should also contain sufficient details for the Ombudsman to assess whether an organization has correctly applied the real risk of significant harm standard and otherwise met its obligations to report and notify in respect of breaches that pose a real risk of significant harm. This could include a brief explanation of why the trustee determined there was not a real risk of significant harm in cases where the trustee did not report the breach to the Ombudsman and notify individuals.

Records should describe the nature or type of information involved in the privacy breach, but need not include personal details unless necessary to explain the nature and sensitivity of the information.

Additional recording requirements for notifications given orally are provided under "**What is direct notification?", above.**

Are there financial penalties?
Yes. Under PHIA, failure to comply with section 19.0.1 (notification of privacy breach) is an offence and doing so could lead to fines.

The Office of the Manitoba Ombudsman does not prosecute offences under PHIA or issue fines. What the Ombudsman can do is refer information relating to the possible commission of an offence to the Department of Manitoba Justice, who would be responsible for any ultimate prosecution.

Who needs to create a process for managing privacy breaches?
All trustees who maintain personal health information about individuals should have a process in place to manage and respond to privacy breaches.

My organization only employs four people. Do I still need to create a process for managing privacy breaches?
Yes. Large and small trustees of personal health information must comply with their obligations under PHIA, including notifying individuals and reporting to the Ombudsman all privacy breaches that create a real risk of significant harm.

What considerations should go into creating a process for managing privacy breaches? Where can I get advice on how to create a process for managing privacy breaches?
Trustees of personal health information should have a process in place for:

(1) Containing a breach,
(2) Evaluating the risks associated with the breach and implementing a pre-determined breach protocol,
(3) Notifying affected individuals and the Office of the Manitoba Ombudsman (if applicable), and
(4) Investigating and preventing further breaches.

Privacy breach guidelines have been prepared by the Manitoba Ombudsman, and are available for anyone to use. The privacy breach guidelines can be found on the Manitoba Ombudsman's website at:

I already have a process for managing privacy breaches. Do I need to change it?
If trustees have a process for managing privacy breaches, they should review it to make sure it meets the new requirements set out under PHIA and its Regulation.

Do I have to file a copy of my process for managing a privacy breach with someone?
No. Trustees should have a process for managing privacy breaches in place, but they do not need to submit their process to anyone for approval. Trustees may consult these guidelines, or the Manitoba Ombudsman's website to obtain more information on managing privacy breaches.

Sometimes I am legally obligated to disclose information. Could this be considered a privacy breach?
Disclosing personal health information in a way that is either permitted or required by

law, which could include disclosing information about infectious diseases to public health officials, does not constitute a privacy breach. Trustees should seek their own legal advice to determine if there is an authority in place to disclose personal health information under PHIA or any other applicable law.

A patient made a disclosure directive that restricts me from sharing information with someone. I accidentally forgot about it and shared their information with another trustee. Is this a privacy breach?

Disclosing an individual's personal health information in a way that is contrary to their instructions may represent a privacy breach, unless the disclosure is otherwise permitted or required by law. Trustees should seek their own legal advice to determine if there is an authority in place to disclose personal health information under PHIA or any other applicable law.