In accordance with Shared Health policy ***Reporting and Investigating Privacy Breaches and Complaints***, individuals affected by a breach of their personal health information must be notified whenever the breach investigation determines the breach has the potential to place the individual at real risk of Significant Harm.

Definitions

CPO – means Shared Health Chief Privacy Officer

Individual – means patient/client/resident

Privacy Breach - means, in relation to personal information,
(a) theft or loss; or
(b) access, use, disclosure, destruction or alteration in contravention of this Act

PO – means site Privacy Officer

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.*

Where real Risk of Significant Harm exists individuals ***must be notified.***

8.7 Notifying individual of Privacy Breach - The following factors are to be considered where there is a real Risk of Significant Harm

(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, having regard for:

(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 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 persons who actually or potentially accessed the personal health information have committed to destroy and not use or disclose the information,

(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; and

(c) any other factors that are reasonably relevant in the circumstances

8.8(1) When notice of a privacy breach is to be given to an individual, the notice must be given in writing and must include the following:

(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 notified about the privacy breach;

(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.

**** When a privacy breach has been determined to be a risk of significant harm, in concert with notification to the individual (please refer to Breach Notification letter template), notification must also be provided to the Manitoba Ombudsman.***

***** The Shared Health and WRHA Chief Privacy Officer must be notified of any breaches resulting in a risk of significant harm so as to ensure that the Ombudsman is notified of same.***

8.8.(2) 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, the Trustee may give the notice orally.

8.8.1(1) When indirect notification may be given, notification of a privacy breach may be given indirectly to one or more individuals in the following circumstances:

(a) If the Trustee reasonably believe that the privacy breach may result in a risk to public health or safety;

(b) If the identity or current contact information of the individual or individuals is not known;

(c) If the Trustee reasonably believe giving notice to an individual in accordance with Section 8.8

(j) Is impractical or unduly expensive because of the large number of individuals that may have been affected by the privacy breach, or

(ii) Could threaten or harm the individual's mental or physician health

8.8.1(2) Notification under this section must be given:

(a) 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

(b) if notice of the privacy breach can be reasonably expected to threaten or harm the recipient's mental or physical health, 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.

Process for Notification of Breaches

Where a privacy breach has been confirmed in accordance with the Reporting and Investigating Privacy Breaches and Complaints policy and the Privacy Breach Investigation Process, the Privacy Officer/Manager/Regional Director/Community Area Director liaises with the Shared Health Chief Privacy Officer and others (as required) to determine whether the breach was willful/targeted, and whether there exists a real risk of significant harm to the individual. For example, if the breach occurs after hours, such as when schedule sheets bearing residence access codes are lost or stolen, the program area will **immediately notify** the individual(s) affected and offer support to change access codes.

Where verbal notification of a breach is identified as being the most appropriate means to notify the individual, the Privacy Officer will document that the person has been notified either verbally or in writing, and this notification shall be recorded appropriately in RL6 by the Privacy Officer.

During regular business hours, the site/program area will liaise with site Privacy Officer. and consult with the Shared Health CPO as needed, to determine who may best notify the individual(s) affected.

The Shared Health CPO may also notify other stakeholders, including but not limited to: Manitoba Health and Seniors Care, or other bodies with statutory responsibility for the discipline of health professionals as designated in S. 1.2 of the Personal Health Information Regulation. http://web2.gov.mb.ca/laws/regs/current/_pdf-regs.php?reg=245/97