

Title: Recording of Security Breaches Related to Personal Health Information Policy

Effective Date: December 1, 2011

1. **PURPOSE:**

- 1.1. To ensure that all complaints, alleged breaches of privacy and security pertaining to the collection, access, use, disclosure, privacy, confidentiality, security and integrity of personal health information including demographic Information are reported, recorded and analyzed in accordance with *The Personal Health Information Act* (“PHIA”).
- 1.2. To ensure that corrective procedures are in place to remedy any confirmed breach of personal health information.

2. **DEFINITIONS:**

- 2.1. Access: The right of an individual (client) or a person permitted to exercise the rights of that individual to examine (view) and receive a copy of the individual’s personal health information maintained by the trustee.
- 2.2. Breach of Security: Occurs whenever personal health information is collected, used, disclosed or accessed other than as authorized, or its integrity is compromised.
- 2.3. Complaint: A complaint made to a trustee by an individual and/or by the provincial ombudsman about collection, access, correction, use, disclosure, protection and privacy of personal health information.
- 2.4. Confidentiality: The obligation of a trustee to protect the personal health information entrusted to it, to maintain the secrecy of the information and not misuse or wrongfully disclose it.
- 2.5. Demographic Information: An individual’s name, address, telephone number, and email address.
- 2.6. Disclosure of Personal Health Information: Revealing the personal health information outside the trustee, such as to other trustees, to family and friends of the individual, or to other persons legally entitled to have personal health information released to them.
- 2.7. Health Care: Any care, service or procedure provided to diagnose, treat or maintain an individual’s health; provided to prevent disease or injury or promote health care; or that affects the structure or a function of the body and includes the sale or dispensing of a drug, device, equipment or other item pursuant to a prescription.
- 2.8. Health Care Facility: A hospital, personal care home, psychiatric facility, medical clinic, laboratory, CancerCare Manitoba and community health centre or other facility in which health care is provided and that is designated in the PHIA regulations.
- 2.9. Health Professional: A person who is licensed or registered to provide health care under an Act of the Legislature or who is a member of a class of persons designated as health professionals in the PHIA regulations.
- 2.10. Health Services Agency: An organization that provides health care such as community or home-based health care pursuant to an agreement with the trustee.
- 2.11. Individual: A person receiving health care services. For the purpose of access, correction, use and disclosure of personal health information includes persons permitted to exercise

the rights of the individual. For clarity, health care services means occupational therapy services provided to clients in any setting.

- 2.12. Integrity of Personal Health Information: The preservation of its content throughout storage, use, transfer, and retrieval so that there is confidence that the information has not been tampered with or modified other than as authorized.
- 2.13. Maintain: In relation to personal health information, to have custody or control of the information.
- 2.14. Personal Health Information: Recorded information about an identifiable individual that relates to:
- the individual's health, or health care history, including genetic information about the individual;
 - the provision of health care to the individual; or
 - payment for health care provided to the individual;
- and includes:
- the PHIN (personal health identification number) and any other identification number, symbol or particular assigned to an individual; and
 - 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.
- 2.15. PHIA: *The Personal Health Information Act* (Manitoba).
- 2.16. PHIN: The personal health identification number assigned to an individual by the minister to uniquely identify the individual for health care purposes.
- 2.17. Personal Representative:
- an executor/executrix or joint executor/executrix named in a deceased individual's will; or
 - court appointed administrator or joint administrator of a person's estate.
- 2.18. Persons Permitted to Exercise the Rights of an Individual includes:
- 2.18.1. (a) any person with written authorization from the individual to act on the individual's behalf;
- (b) a proxy appointed by the individual under *The Health Care Directives Act*;
- (c) committee appointed for the individual under *The Mental Health Act* if the committee has the power to make health care decisions on the individual's behalf;
- (d) a substitute decision maker for personal care appointed for the individual under *The Vulnerable Persons Living with a Mental Disability Act* if the exercise of the right relates to the powers and duties of the substitute decision maker;
- (e) the parent or guardian of an individual who is a minor, if the minor does not have the capacity to make health care decisions;
- (f) if the individual is deceased, his or her personal representative.

2.18.2. If it is reasonable to believe that no person listed in any clause of 2.15.1 exists or is available, the adult person listed first in the following who is readily available and willing to act may exercise the rights of an individual who lacks the capacity to do so:

- (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.

Ranking: The older or oldest of two or more relatives described in any clause of 2.15.2 is to be preferred to another of those relatives.

2.19. **Privacy:** The fundamental right of the individual to control the collection, use and disclosure of their personal health information.

2.20. **Record or Recorded Information:** A record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, on any storage medium or by any means, including by graphic, electronic or mechanical means, but does not include electronic software or any mechanism that produces records.

For clarity, a record means information, however recorded (e.g. written, audio, video, computer disk), generated by the occupational therapist or an person supervised by the occupational therapist. This includes but is not limited to assessments and evaluations, therapy goals, progress toward goals, attendance and remuneration records. When the record belongs to the occupational therapist it may also include items not generated by the occupational therapist such as, but not limited to, a referral, correspondence, and reports prepared by others.

2.21. **Representative:** In relation to an individual, means persons permitted to exercise the rights of an individual.

2.22. **Security:** The process of protecting the personal health information by assessing threats and risks to information and taking steps to mitigate these threats and risks. The result is the consistent application of standards and controls to protect the integrity and privacy of the information during all aspects of its use, processing, disclosure, transmittal, transport, storage, retention including conversion to a different medium and destruction.

2.23. **Trustee:** A health professional, health care facility, public body, or health services agency that collects or maintains personal health information. For clarity, an occupational therapist is a trustee under the PHIA if he or she is a registered occupational therapist and is self employed or employed by a non-trustee. Health professionals employed by a trustee, such as a hospital government agency, etc are not considered trustees; however as employees of these facilities, occupational trustees must comply with the PHIA.

- 2.24. Use: Involves revealing personal health information to someone within the trustee's own organization who needs to know the information to do their job. Use includes processing, reproduction, transmission and transportation of personal health information.

3. POLICY:

- 3.1. A trustee who receives a complaint, or has knowledge of or reasonably believes that an alleged breach of security has occurred shall immediately record the incident. (Section 2 of Regulation 245/97)
- 3.2. The trustee may determine whether to proceed with an investigation of the complaint and/or alleged breach of security based on the results of the analysis taking into consideration:
- the length of time that has elapsed since the date the subject matter of the complaint arose makes the investigation no longer practicable or desirable;
 - the subject matter of the complaint is trivial or the complaint is not in good faith or is frivolous or vexatious;
 - the circumstances of the complaint do not require investigation.
- 3.3. If the decision is made to proceed with an investigation the trustee shall investigate the allegation (this process will include obtaining the alleged violator's version of events), consult with the appropriate resources, document findings and make a determination as to whether a breach has occurred.
- 3.4. If it is determined that a breach of personal health information has occurred corrective procedures to address the security breached shall be taken. (Section 2 of Regulation 245/97)
- 3.5. When a breach has occurred the trustee shall determine whether any of the following should be notified:
- the individual(s) the information is about;
 - the office of the ombudsman;
 - the College of Occupational Therapists of Manitoba;
 - the media.

4. PROCEDURE:

- 4.1. Record the incident;
- 4.2. Consult with the appropriate authorities (internal and external) and take appropriate action;
- 4.3. Determine the corrective action to be taken.

5. REFERENCES:

- 5.1. *The Personal Health Information Act.*
- 5.2. *Personal Health Information Regulation.*

Reporting of Security Breaches Related to Personal Health Information Policy –Guidelines

The standard operating procedure for reporting of security breaches related to personal health information at this company is:

1. Any complaints and/or alleged breaches of security are documented.
2. Any complaints and/or alleged breaches analyzed to determine whether to proceed with an investigation.
3. If the decision is made to proceed with an investigation consultation takes place with appropriate resources when required, findings are documented and it is determined whether a breach has occurred.
4. If it is determined that a breach has occurred appropriate corrective procedures are taken and where necessary notification occurs.

For further clarification on any point, please refer to the full policy.