Title: Security and Storage of Personal Health Information Policy
Effective Date: December 1, 2011

---

1. **PURPOSE:**

1.1. To ensure personal health information, demographic information, and personal information regardless of media (electronic form, paper form, etc) is properly stored in a secure environment.

1.2. To ensure that security and integrity measures are in place to protect the confidentiality and integrity of personal health information demographic information and personal information.

1.3. To ensure the security and integrity of the information during transmittal by any means including by internal and external delivery networks, voice mail, wireless technology, email and the internet.

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. 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.

2.4. Demographic Information: An individual's name, address, telephone number, and email address

2.5. 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.

2.6. Eligibility Information:

- Name;
- Signature;
- Address;
- Telecommunications information;
- Sex;
- Date of birth;
- Date of death;
- Family associations;
- Eligibility for health care coverage;
- Jurisdiction of residence;
- Manitoba Health family registration number;
- Personal Health Information Number (PHIN);

- A unique identifier equivalent to the PHIN assigned by another jurisdiction that pays for health care;
- A unique identifier assigned by a trustee, when accessed by that trustee;
- A non-Canadian health identification number.

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. Information Manager: A person or body (corporation, business, or association) that processes, stores or destroys personal health information or provides information management or information technology services for the trustee.

2.13. 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.

2.14. Maintain: In relation to personal health information, to have custody or control of the information.

2.15. Personal Digital Assistants (PDAs): includes wireless devices such as Blackberries, iPhones or Palm Pilots that provide organizer capabilities, and access through synchronization to email, calendar and internet functionality.

2.16. 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.

2.17. PHIA: *The Personal Health Information Act* (Manitoba).

2.18. PHIN: The personal health identification number assigned to an individual by the minister to uniquely identify the individual for health care purposes.

2.19. Personal Information: Information about an identifiable individual that is recorded in any form such as:

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual;
(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
(c) any identifying number, symbol or other particular assigned to the individual;
(d) the address, fingerprints or blood type of the individual.

But does not include the name, title or business address or telephone number of an employee of an organization.

2.20. 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.

2.21. Persons Permitted to Exercise the Rights of an Individual includes:

2.21.1. (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.

2.21.2. 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.

2.22. PIPEDA*: The Personal Information Protection and Electronic Documents Act* (Canada).

2.23. Portable Electronic Devices: Includes all mobile computing devices used to store personal health information or personal information. Examples include but are not limited to:

- laptop/notebook computers;
- personal digital assistants;
- cellular phones; and
- removable storage devices.

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

2.25. 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 a person supervised by the occupational therapist. This includes but is not limited to assessments and evaluations, therapy goals, progress towards 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.

2.26. Record of User Activity: A record about access to personal health information maintained on an electronic information system, which identifies the following:

- individuals whose personal health information has been accessed,
- persons who accessed personal health information,
- when personal health information was accessed,
- the electronic information system or component of the system in which the personal health information was accessed,

whether personal health information that has been accessed is subsequently disclosed under section 22 of PHIA.

2.27. Removable Storage Devices (Electronic Storage Media): Includes diskettes, magnetic tape, CD ROMS, disk drives, laser disks and any small portable memory card or drive that plugs into any computer's USB port and can function as a storage device or a portable hard drive. Examples of removable storage devices include but are not limited to Universal Serial Bus (USB Drive), iPods, Zip Drive, Flash Drive, or Tokens.

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

2.29. Secured Place: A physical environment for the storage or handling of personal health information that includes the applicable following characteristics:

- not readily accessible by unauthorized users;
- supervised or monitored by authorized users;
- keyed to allow entrance to authorized users only;
- locked when authorized users are not in attendance;
- protected by controls to minimize loss, destruction or deterioration caused by fire, water, or humidity damage; and
- proper containers and adequate labeling are used to reduce accidental loss or destruction.

2.30. 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.

2.31. 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.

2.32. 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 shall ensure that recorded personal health information will be maintained in designated areas and properly secured in the appropriate manner to protect its confidentiality, security, accuracy and integrity. (Section 18(1) and Section 3 of Regulation 245/97)

3.2. Security safeguards shall include both physical and human resource safeguards to prevent unauthorized personal health information collection, use, disclosure and access. Section 18(1)

3.3. Physical security measures include such safeguards as locked filing cabinets, restricted access to certain offices and designated areas, the use of passwords, encryption. Human resource aecurity measures include aecurity clearances, sanctions, training and contracts. (Section 3 of Regulation 245/97)

3.4. All written personal health information shall be placed in an appropriately secured file. Paper files containing such information shall be kept in a secured place at all times other than when being updated or used by authorized personnel as a necessary function of their work.

3.5. All personal health information that is mailed through regular postal service, interdepartmental mail or sent via courier must be marked confidential and have reasonable safeguards put in place to ensure security and integrity of the information. Section 18(1)

3.6. A trustee who maintains personal health information in electronic form shall create and maintain or have created and maintained a record of used activity for any electronic system it uses to maintain personal health information. (Section 4(1) of Regulation 245/97)

3.7. A trustee shall audit records of user activity to detect security breaches. (Section 4(4) of Regulation 245/97)

3.8. A trustee shall maintain a record of user activity for at least three years. (Section 4(5) of Regulation 245/97)

3.9. A trustee shall ensure that at least one audit of a record of user activity is conducted before the record is destroyed. (Section 4(6) of Regulation 245/97)

3.10. Portable electronic devices shall not be used to collect or store personal health information about individuals receiving health care services unless:

a) The information saved to the device is encrypted;
b) The device is password protected;
c) All reasonable steps are made to de-identify the information, where possible, prior to saving it to the device;
d) The device is not left unattended or in an unsecured location;
e) Appropriate precautions are taken to prevent loss or theft of the device;
f) Information contained on the device is not subject to unauthorized access;
g) Any information stored on the devise is subjected to weekly back-ups and not stored on the device for long periods of time.

3.11. Personal health information stored in electronic form shall be properly secured from unauthorized access. Personal health information stored on portable electronic devices or removable storage devices shall be kept in a secured place at all times and shall be used only by authorized personnel. (Section 3 of Regulation 245/97)

3.12. Personal Health Information shall not be transmitted via electronic mail without appropriate safeguards such as encryption or transmittal within a secure firewall where practicable. (Section 3 of Regulation 245/97)

3.13. If personal health information is removed from the trustee's premises by an authorized person that person(s) shall carry the file/electronic media with them or ensure secure storage at all times. If it is necessary to leave personal health information unattended in

a vehicle, it must be stored in a secured place (such as a locked trunk or in an out-of-sight location in a locked vehicle if there is no trunk). Section 18 (1)

3.14. Everyone dealing with personal health information in any manner shall take reasonable precautions to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction or loss and any other hazards. (Section 3 of Regulation 245/97)

3.15. No personal health information shall be transported, stored or left in a location that could result in the destruction or deterioration of the personal health information. (Section 3 of Regulation 245/97)

3.16. Any agent retained to transport or deliver any personal health information shall be advised in writing of the conditions necessary for the safe transport of the personal health information. For example, any service contract for the transport or delivery of personal health information shall contain:

- a provision advising the service provider of the requirements to safeguard the confidentiality of personal health information and to physically protect it from unintended destruction;
- an agreement by the service provider that it and its employees or agents shall protect the confidentiality, security and physical integrity of personal health information.

3.17. All personal health information shall be disposed of or destroyed in such a way that it cannot be reconstructed or retrieved, by supervised incineration, shredding or in accordance with industry standards. Section 17(3)

3.18. All hard drives and other electronic media shall be physically destroyed or wiped clean of all data and software. Section 17(3)

3.19. Office machines such as photocopiers, fax machines, scanners and printers contain hard drives that must be overwritten, removed and destroyed when machines are replaced. Section 17(3)

4. PROCEDURE:

4.1. A record of user activity may be generated manually or electronically**.** (Section 4(2) of Regulation 245/97)

4.2. A record of user activity is not required if the personal health information is demographic information or eligibility information, or is disclosed under section 22(2)(h) of the Act or is accessed while generating, distributing or receiving reports. (Section 4(3) of Regulation 245/97)

5. REFERENCES:

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

Security and Storage of Personal Health Information Policy –Guidelines

The standard operating procedure for securing and storing personal health information at this company is:

1. Personal health information is maintained is designated areas and files are locked in filing cabinets.
2. All written personal health information is placed in an appropriately secured file.
3. All personal health information that is mailed through regular postal service, interdepartmental mail or sent via courier is marked confidential.
4. When personal health information is maintained in an electronic system a record of used activity is created and maintained for three years.
5. Audits are conducted on a regular basis to detect security beaches.
6. Portable electronic devices used to store personal health information are encrypted password protected, not left unattended and kept is a secure location.
7. Any information stored on a portable electronic device is subjected to weekly back-ups and not stored on the device for long periods of time.
8. When personal health information is removed from our premises files and/or electronic media are kept with the person.
9. If personal health information must be left unattended in a vehicle, it is stored in a locked trunk or in an out-of-sight location in a locked vehicle if there is no trunk.
10. No personal health information is transported, stored or left in a location that could result in the destruction or deterioration of the information.
11. All personal health information is destroyed by shredding it.
12. All hard drives and other electronic media are wiped clean of all data and software before they are disposed of.

13. Office machines such as photocopiers, fax machines, scanners and printers contain hard drives and are overwritten; removed and destroyed when machines are replaced.

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