Winnipeg Regional Health Authority / Office régional de la santé de Winnipeg — Caring for Health / À l'écoute de notre santé	**REGIONAL** Applicable to all WRHA governed sites and facilities (including hospitals and personal care homes), and all funded hospitals and personal care homes. All other funded entities are excluded unless set out within a particular Service Purchase Agreement.		Level: 1
POLICY	Policy Name: **Security and Storage of Personal Health Information**	Policy Number: 10.40.120	Page 1 of 5
	Approval Signature: *Original signed by B. Postl*	Section: GENERAL ADMINISTRATION	
	Date: February 2008	Supercedes: May 31, 2000	

1.0 PURPOSE:

1.1 To ensure personal health information, regardless of media (electronic form, paper file, or radiological/digital image) is properly stored in a secure environment.

1.2 To ensure that security and integrity measures are in place and followed in order to protect the confidentiality and integrity of personal health information within the Winnipeg Regional Health Authority ("WRHA").

1.3 To ensure the security and integrity of personal health information during transmittal by any means including by internal and external delivery networks, voice mail, wireless technology, e-mail and the Internet.

2.0 DEFINITIONS:

2.1 Secured Place means a physical environment for the temporary or permanent storage of, or for the use, processing or transmittal of personal health information that has the 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.

2.2 Security means the consistent application of standards and controls to protect the integrity and privacy of personal health information during all aspects of its use, processing, disclosure, transmittal, transport, storage, retention, including conversion to a different medium, and destruction.

2.3 Integrity of Personal Health Information means 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.

2.4 A Breach of Security occurs whenever personal health information is collected, used, disclosed or accessed other than as authorized, or its integrity is compromised.

2.5 Information Systems Designate ("IS Designate") means the individual with expertise in information systems and technology designated by the Vice-President, Finance to work with the Privacy Officer to develop policies and procedures to safeguard and audit the confidentiality and integrity of personal health information stored, processed or transmitted electronically.

3.0 POLICY:

3.1 The WRHA as a trustee of health information under *The Personal Health Information Act* ("PHIA") shall ensure that recorded personal health information will be properly secured and maintained in the appropriate manner to protect its confidentiality and integrity. Recorded personal health information includes information that is written, photographed, recorded or stored in any manner, on any medium or by any means, including by graphic, electronic, audio, radiological, digital or mechanical means.

3.2 Personal health information is to be collected, used, disclosed or accessed only by individuals who are authorized for that purpose. Individuals thus authorized must have a clear understanding of the authority, parameters, purposes and responsibilities of their access, and of the consequences of failing to fulfill their responsibilities.

3.3 Security safeguards shall include both physical and human resource safeguards to prevent unauthorized personal health information collection, use, disclosure and access.

3.4 Physical security measures include such safeguards as locked filing cabinets, restricted access to certain offices or areas, the use of passwords, encryption and lock-boxes. Human resource security measures include security clearances, sanctions, training and contracts.

3.5 Security safeguards should incorporate appropriate identification, authentication and information integrity/availability as appropriate.

4.0 PROCEDURE:

4.1 WRHA Employees and Persons Associated with the WRHA

4.1.1 All written personal health information shall be placed in an appropriately secured file. Paper files (both patient and employee) containing such information shall be kept in a secure place at all times within the resources available other than when being updated or used by authorized personnel as a necessary function of their work.

4.1.2 Personal health information stored in electronic form on a fixed computer server or terminal shall be properly secured from unauthorized access. Personal health information stored on electronic media (diskettes, magnetic tape, CD ROM'S, disk drives, laser disks, etc.) shall be kept in a Secured Place at all times and shall be used only by authorized personnel having access to a protected system. Prior to removal from an

office, any personal health information contained within the computer hardware or on electronic storage media shall be secured or removed.

4.1.3 Individuals who sign on to a computer must not leave the computer on in accessible areas when they leave their workstation. User password protocols must be in place and utilized. Where possible, automatic shut offs after a prescribed period of disuse should be programmed for all workstations.

4.1.4 Radiological and digital images shall be appropriately labeled and kept in a Secured Place at all times other than when required for work purposes by authorized personnel.

4.1.5 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.

4.1.6 Personal health information shall not be transmitted via electronic mail without appropriate safeguards such as encryption or transmittal within a secure firewall where practicable.

4.1.7 Persons leaving voice messages containing personal health information should be discreet. Personal health information should never be left on a patient's voicemail unless the individual whom the information is about has authorized it. Any personal health information relayed by voice message should be kept to the minimum required for the purpose of the communication. Persons receiving voice messages containing personal health information should listen to the message in private, and delete the message as soon as possible. Appropriate passwords and security measures should be in place for access to voice mail.

4.1.8 Fax machines shall be located in a Secured Place where they can be used and monitored only by authorized persons. A cover sheet, with approved WRHA logo, should be attached to all documents stating that the transmittal is confidential and that any unintended receiving party is prohibited from reading or disclosing the information to anyone else (i.e. a Confidentiality Caution). Users of fax machines shall follow the *WRHA Policy: Transmission of Personal Health Information by Facsimile*.

4.1.9 If personal health information is removed from the trustee's premises by an authorized person for purposes authorized by the trustee, 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). All personal health information removed from a secure office location shall be recorded in tracking system.

4.1.10 Personal health information files/electronic media shall be returned to its designated and secured storage location and not allowed to accumulate or be left unattended on desktops or any other location in a non-secured place.

4.1.11 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.

4.1.12 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. For example, radiological images or computer disks could be destroyed if left in a locked trunk on a hot day; paper records could be destroyed if left by an open window during a rainstorm.

4.2 **Manager/Supervisor**

4.2.1 The manager/supervisor shall ensure that all employees be made aware of the policy respecting security and storage of personal health information.

4.2.2 Managers/supervisors shall review practices of employees to ensure these standards are being maintained and that there are no breaches of security.

4.2.3 When standards are not being maintained or when a security breach occurs, such situations shall be brought to the attention of the Privacy Officer, recorded and corrective steps taken. An occurrence report should be forwarded to the Privacy Officer, or designate.

4.2.4 If personal health information is perishable in certain conditions, any agent retained to transport or deliver any personal health information for the WRHA shall be advised in writing of any specific information regarding the perishability of the information and 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, including any appropriate cautions as to the perishability of the particular media used for the personal health information in question.

- 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.

4.3 **Privacy Officer/Designate**

4.3.1 Conduct periodic surveys of building security with regard to potential for unauthorized access to personal health information.

4.3.2 Ensure provision is made for confidential materials to be stored in a Secured Place.

4.3.3 Work in collaboration with the IS Designate to ensure the security of personal health information processed, stored or transmitted electronically.

4.3.4 Keep a log of breaches of security and, in conjunction with the IS Designate, prepare a report for the Chief Executive Officer detailing any breaches of security and any corrective and disciplinary procedures instituted.

4.4 **IS Designate**

4.4.1 To ensure appropriate procedures and safeguards are in place to safeguard the confidentiality, security and integrity of personal health information used, processed, stored or transmitted electronically.

4.4.2 Work in collaboration with the Privacy Officer to ensure the security of personal health information in an electronic format.

4.4.3 Keep a log of breaches of security in conjunction with the Privacy Officer and prepare a report for the Chief Executive Officer detailing any breaches of security and any corrective and disciplinary procedures instituted.

5.0 LEGISLATIVE REFERENCES:

- *The Personal Health Information Act*, Personal Health Information Regulation (245/97), Registered December 11, 1997, Section 2.
- *The Personal Health Information Act*, Division 2, 18(1), 18(2).
- The Canadian Medical Association Health Information Privacy Code, 1998.

Policy Contact: *Landis Esposito, Chief Privacy Officer*