CATEGORY:	**ORGANIZATIONAL: INFORMATION TECHNOLOGY**
SUB-CATEGORY:	**APPROPRIATE TECHNOLOGY USE**
GROUP:	
DISTRIBUTION:	**ALL STAFF / PHYSICIANS**
TITLE:	**SECURITY OF CONFIDENTIAL INFORMATION**

PURPOSE

To provide guidelines with respect to the protection of confidential, private and/or personal information/personal health information relating to clients/patients/residents, employees and/or the business of Western Health, in an effort to:

- prevent unauthorized access to such information;
- eliminate risks associated with malicious exposure of, or damage to, computer systems;
- eliminate risks related to unauthorized collection, use and disclosure of confidential, private and/or personal information/personal health information;
- protect the privacy of users and providers of health services; and
- adhere to all legislation governing personal information/personal health information created and received by Western Health pursuant to its mandate.

POLICY

Security of confidential, private and/or personal information/personal health information relating to clients/patients/residents, employees and the business of Western Health is a priority for the organization. All employees and other affiliates of Western Health who collect, use, disclose or destroy confidential information for any purpose must adhere to the organization's information security policies, procedures and practices.

Western Health must develop, sustain and protect the integrity of the information generated within its service delivery and organizational processes through the use of administrative, technical and physical safeguards.

Any misuse of confidential information, including failure to protect information in one's custody and control, is considered a breach of confidentiality and may result in disciplinary action up to and including:

- termination of my employment / contract for service
- reporting to an individual's professional Association / College
- civil action / criminal prosecution.

For additional information, please refer to Western Health's policy 2-03-10 *Confidentiality.*

All copies of personal information / personal health information or other confidential information are subject to the same protection and controls as the original documents.

Notwithstanding the physical configuration of facilities and service delivery processes, every reasonable effort must be made to ensure that personal information / personal health information and other confidential information is:

- protected against theft, loss and unauthorized access, use or disclosure;
- protected against unauthorized copying, damage or modification; and
- retained, transferred and disposed of in a secure manner.

The following is a non-exhaustive list of preventative measures to maintain the security of confidential information:

1. Confidential information must not be located on desktops where other clients/patients/residents or unauthorized individuals may view the information. It is recommended that, at the very least, this information be contained in a folder which can be closed on the desk when being approached by unauthorized individuals.

2. Confidential information being transported, transmitted, accessed, or otherwise in active use by an authorized person must be in the immediate care and control of this individual, who is responsible for protecting the information from unauthorized viewing or access. Wherever possible, confidential information must not be left in a vehicle. Where this must take place, information must be hidden from view in a locked vehicle.

3. All paper documents containing confidential information must be placed in envelopes or folders prior to being placed in an area that might be "open" to individuals who need not have access to this information, such as mailboxes, mail rooms, Outpatient Department clinics, hospital units, etc.

4. Client/patient/resident records must be returned to their secure location as soon as possible once services have been provided (preferably the same day).

5. All means reasonably available must be used to secure personal information/personal health information. These means must include, but are not limited to:
   - locking filing cabinets containing confidential information when not in use (i.e. at the end of the day or when leaving the area for an extended period of time), or otherwise;
   - locating these cabinets in a secure area, and
   - as existing cabinets are replaced, include locking mechanisms.

6. Client/patient/resident records must not to be removed from Western Health facilities except in accordance with applicable organizational policies, as necessary for providing care/service off site in a community setting, or as required by law, while considering that:
   - only the minimum information required for the authorized use will be permitted to be removed;
   - original documents may only be removed when copies are not practical. In cases where copies are made, where possible, all copies must be destroyed once they are no longer in use;
   - client/patient/resident records may only be removed in consultation with the Health Records Department or program manager or designate in areas where records are not managed by the Health Records Department;
   - once removed, client records must be secured at all times by the individual responsible for removing the information; and
   - client/patient/resident records must be returned to their secure area at first opportunity (preferably the same day).

7. When not in active use, confidential information must be kept in a secure environment, such as a locked filing room, filing cabinet, or other designated area for securing physical client information. When unlocked and in use, these areas must be supervised by authorized individuals, assuring confidentiality and control of the information at all times.

8. Where applicable, all paper-based personal information/personal health information must be signed out of a storage area by an authorized person.

9. Clinical areas must be restricted to employees who require access to the area for the completion of their work responsibilities. All other activity must be kept at a minimum.

10. Confidential information must not be left on answering machines if this practice can be avoided, or unless you have specific client/patient/resident consent to do so (refer to *Guidelines for Leaving Messages Containing Personal Health Information on Telephone Answering Systems*, as available on the Access and Privacy page on Western Health's intranet.

11. Discussions of confidential information must not occur in public areas. When the discussion of confidential information is required in a public area due to an operational or service delivery emergency, extreme caution must be exercised.

12. Discussions of confidential information must occur on a "need to know" basis only.

13. Measures to authenticate the identity of the individual to whom confidential information is being disclosed must be considered prior to the disclosure of such information.

14. Fax machines and printers must be located in secure areas and every effort must be made to immediately remove confidential information from shared printers or fax machines.

15. All e-mail or facsimile communications must include the approved Western Health confidentiality clauses (refer to policy 9-01-10 *Faxing Information*) stating that:
    - The information is confidential and intended only for the recipient;
    - Instructions to delete or shred any information obtained in error; and
    - Include contact information with a request to notify the sender immediately if received in error.

16. Electronic confidential information must be protected within Western Health information management practices, policies and procedures.

17. Access to electronic confidential information must be limited to authorized employees, care/service providers or other authorized users and will be accessible only with the use of proper user names and passwords. Access audits will be performed as required.

18. Electronically-stored confidential information must be protected via privacy-enhancing technologies such as encryption, access controls, routine audits and firewalls. Subject matter experts (i.e. IM; privacy staff) must be consulted to determine the appropriate methodologies for protecting electronically-stored confidential information.

19. Mobile wireless devices must not be left in places where they may be at risk of unauthorized access or theft. In particular, when confidential information in electronic format is being stored or transported on a device that is not connected to the Western Health network (e.g. laptop computer, USB), the user must contact the helpdesk to ensure that proper encryption is in place. (Please refer to policy 5-01-30 *Usage of Western Health Owned Cell Phones and Blackberries*.)

20. Computer monitors must have features such as privacy screens, screensavers and timeout mechanisms, or be situated to prevent the information on the screen from being viewed by unauthorized individuals.

21. Computer passwords must not be shared and it is not recommended that they be written down (refer to policy 10-01-20 *Auditing Access to Electronic Personal Health Information*.)

22. Unauthorized individuals must not access confidential information for reasons unrelated to performing their assigned duties. (Please refer to policy 10-01-20 *Electronic Health Record User Access Review*).

23. Any printed materials containing personal health information that is not required to be placed on a client's record or other file (e.g. appointment books) must be securely stored or disposed of in a Western Health confidential waste bin when the information is no longer needed.

DEFINITIONS

Affiliate: For the purpose of this policy, affiliate is a term used to describe physicians, agents, contractors, volunteers, and health care professionals who have the right to treat persons at a health care facility operated by the custodian.

Agent: In relation to a custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian. Students are covered under this definition.

Confidential Information: All personal information / personal health information of clients/patients/residents and employees as well as the confidential business of Western Health.

Confidential Business Information: Information with respect to Western Health's business that is not publicly disclosed by the organization. Employees / affiliates may come in contact with such information that is not generally known to the public as they perform their duties. Examples include:

- Legal matters involving the organization that are not public knowledge,
- Financial information that is not available in Western Health's annual report,
- Contractual agreements with vendors, consultants, contractors, and third parties (The confidentiality of this information may be written into the contract, eg. non-disclosure of the cost of the service),
- Information about intellectual property such as development of new technology and treatments or unpublished reports,
- Information pertaining to Western Health's information technology access and security systems such as:
    - Information that could lead to inappropriate access to internal and external computer resources,
    - Information that is regarded as confidential between the vendor and Western Health related to negotiated product discounts,
    - Products that are part of Western Health's security infrastructure or the names of vendors of hardware / software solutions that may be vulnerable to external access attacks.

Health Care Professional: A person, including a corporation, that is licensed or registered to provide health care by a body authorized to regulate a health care professional under one of the following enumerated Acts but does not include an

employee of a health care professional when acting in the course of his or her employment:

(i) *Chiropractors Act*,

(ii) *Dental Act*,

(iii) *Denturists Act*, 2005,

(iv) *Dieticians Act*,

(v) *Dispensing Opticians Act*, 2005,

(vi) *Hearing Aid Practitioners Act*,

(vii) *Licensed Practical Nurses Act*, 2005,

(viii) *Massage Therapy Act*, 2005,

(ix) *Medical Act*, 2005,

(x) *Occupational Therapists Act*, 2005,

(xi) *Optometry Act*, 2004,

(xii) *Pharmacy Act*,

(xiii) *Physiotherapy Act*, 2006,

(xiv) *Psychologists Act*, 2005,

(xv) *Registered Nurses Act*, and

(xvi) *Social Workers Association Act*

Health Care Facility: A facility that provides in-patient health care, including a hospital, a psychiatric unit under the *Mental Health Care and Treatment Act*, a personal care home, a community care home, a long-term care home or other facility designated in the regulations.

Personal Information: As defined in the *Access to Information and Protection of Privacy Act* (*ATIPP*), recorded information of an identifiable individual, but does not include the name, title, business address / telephone number of an employee.

(i) the individual's name, address or telephone number,
(ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
(iii) the individual's age, sex, sexual orientation, marital status or family status,
(iv) an identifying number, symbol or other particular assigned to the individual,

(v) the individual's fingerprints, blood type or inheritable characteristics,
(vi) information about the individual's health care status or history, including a physical or mental disability,
(vii) information about the individual's educational, financial, criminal or employment status or history,
(viii) the opinions of a person about the individual, and
(ix) the individual's personal views or opinions.

Personal Health Information: As defined in the *Personal Health Information Act* (*PHIA*), means identifying information in oral or recorded form about an individual that relates to

a) the physical or mental health of the individual, including information respecting the. individual's health care status and history and the health history of the individual's family;
b) the provision of health care to the individual, including information respecting the person providing the health care;
c) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;
d) registration information;
e) payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;
f) an individual's entitlement to benefits under or participation in a health care program or service;
g) information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;
h) a drug as defined in the Pharmacy Act , a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or
i) the identity of a person referred to in section 7.

LEGISLATIVE CONTEXT

Province of Newfoundland and Labrador (2008). *Personal Health Information Act*, SNL 2008, c. P-7.01. Retrieved from http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

Province of Newfoundland and Labrador (2002). *Access to Information and Protection of Privacy Act*, SNL 2002, c. P-7.01. Retrieved from http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

GUIDELINES

Health Information Privacy Initiative (HIPC)-Newfoundland & Labrador: Guidelines for Leaving Messages Containing Personal Health Information on Telephone Answering Machines.

REFERENCES

Eastern Health (2010). *Security of Patient/Resident/Client Personal Health Information*, RM-CR(VI)-100. Retrieved from http://www.easternhealth.ca/?aspxerrorpath=/New/DownFile.Aspx

Province of Newfoundland and Labrador (2010). *The Personal Health Information Act Policy Development Manual*. Retrieved from http://www.health.gov.nl.ca/health/PHIA/PHIA_Policy_Development_Manual_Feb_2011.pdf

Health Information Privacy Collaborative (HIPC) Newfoundland and Labrador (2011), *Guidelines for Leaving Messages Containing Personal Health Information on Telephone Answering Systems.*

KEYWORDS

Security, securing personal health information, confidential information

TO BE COMPLETED BY QUALITY MANAGEMENT & RESEARCH STAFF ONLY

Approved By: Chief Executive Officer	Maintained By: Regional Manager, Information Access & Privacy
Effective Date: 27/January/2014	❒ Reviewed: ☑ Revised: 03/September/2014
Review Date: 03/September/2017	❒ Replaces: *(Indicates name and number of policy being replaced)* OR ☑ New