Labrador-Grenfell Health

SUBJECT: **SECURITY OF CONFIDENTIAL INFORMATION**

APPROVED BY: Chief Executive Officer _____
EFFECTIVE DATE: 2011 10
REVIEW/REVISED DATE:

Purpose:

To provide guidelines regarding the protection of confidential, private and/or personal information relating to clients, employees and/or the business of Labrador-Grenfell 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;
- protect the privacy of users and providers of health services; and
- adhere to all legislation governing personal health information created and received by Labrador-Grenfell Health pursuant to its mandate.

Policy/Standard:

Security of confidential, private and/or personal information relating to clients, employees and the business of Labrador-Grenfell Health is a priority for the organization. Therefore, it is the responsibility and obligation of all employees and other affiliates of the Authority who collect, use, disclose or destroy confidential information for any purpose to adhere to the organization's information security policies, procedures and practices, in order that the integrity of such information is maintained.

Labrador-Grenfell Health is both legally and ethically responsible to 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.

All copies of personal health 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 health 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 should not be located on desktops where other clients or unauthorized persons 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 persons.

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.

3. All paper documents containing confidential information should be placed in envelopes or folders prior to being placed in an area that might be “open” to persons who should not have access to this information, such as mailboxes, mail rooms, OPD clinics, hospital units, etc.

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

5. All filing cabinets containing confidential information must be locked when not in use (i.e. when at the end of the day or when leaving the area for an extended period of time), or otherwise, these cabinets must be located in a secure area. As existing cabinets are replaced, locking mechanisms are considered a required feature.

6. Client records are not to be removed from Labrador-Grenfell Health facilities except in accordance with 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;
- client records may only be removed in consultation with the Health Records Department, program manager or designate (as applicable);
- once removed, client records must be secured at all times by the person responsible for removing the information; and
- client 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. All paper-based personal health information must be signed out of a storage area by an authorized person.

9. Clinical areas should 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 should not be discussed over a phone that may not be secure. It is recognized that there may be times when operational or service delivery emergencies require the use of whatever calling mechanism is available; however, extreme caution must be exercised in such instances.

11. Confidential information should not be left on answering machines if this practice can be avoided, or unless you have specific client consent to do so (refer to *Guidelines for Leaving Messages Containing Personal Health Information on Telephone Answering Systems*, as available on the Labrador-Grenfell Health Intranet).

12. Discussions of confidential information should 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.

13. Discussions of confidential information should occur on a "need to know" basis only.

14. 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.

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

16. All e-mail or facsimile disclosures must include the approved Labrador-Grenfell Health confidentiality clauses (refer to IM&T-8-60 *"Faxing of Confidential 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.

17. Electronic confidential information must be protected within Labrador-Grenfell Health information management practices, policies and procedures.

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

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

20. Mobile wireless devices must not be left in places where they may be at risk of unauthorized access or theft (refer to IM&T-8-20 *"Laptop and Mobile Data Device Policy and Agreement"*).

21. 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 persons.

22. Computer passwords must not be shared and should not be written down (refer to IM&T-8-40 *"Declaration of Responsible Use of Network/Computer Systems").*

23. Unauthorized persons must not access confidential information for reasons unrelated to their employment or clinical role (i.e. unauthorized access to test results, electronic or paper-based, for family/friends is strictly prohibited).

24. Any printed materials containing personal health information that is not required to be placed on a client's record or other file (i.e. appointment books) must be shredded or securely stored when the information is no longer needed.

Related Policies:

• Privacy and Confidentiality	P&A-9-010
• Oath/Affirmation of Confidentiality	P&A-9-020
• Laptop and Mobile Data Device Policy and Agreement	IM&T-8-020
• Faxing of Confidential Information	IM&T-8-060
• Preservation of Communications Pertaining to Adverse Events	PS&Q-5-045

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*.

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