SOP Number:	**125.10**	
Title:	**Privacy and Confidentiality**	
Version Number	Effective Date	Changes
125.10	15 August 2023	Reviewed

Directors Signature: _____ Date: 2023/SEP/01

1. SCOPE

This SOP describes the importance of privacy and confidentiality of all volunteers, patients, and employees.

a. LEGISLATION

PIPEDA

- **P**ersonal **I**nformation **P**rotection and **E**lectronic **D**ocuments **A**ct-legislated on January 1st 2004.
- This legislation governs the collection, use, disclosure, and retention of personal information in the course of commercial activities.
- Personal information includes name, date of birth, address, Health Card Number, and extended health insurance numbers.

PHIPA

- **P**ersonal **H**ealth **I**nformation **P**rotection **A**ct-Ontario enacted on Nov 1, 2004.
- This act provides direction to all individuals who collect, use, disclose, and retain personal information and personal health information.
- Personal Health Information includes any information relating to previous health issues, the records of visits to the hospital, and the health care provided for those visits.

Privacy

- Is the right of an individual to control his or her own personal information.
- A person can determine how, when, and to what extent they will share their information with anyone.

Confidentiality

- Is the obligation of staff and anyone who has access to a person's information to protect information entrusted to them regardless of format; including, but not limited to, verbal, written, and electronic.

Failure to maintain confidentiality may result in disciplinary action, including:

- Loss of privileges
- Loss of affiliation
- Reporting to your professional college
- Civil action
- Criminal prosecution
- Fines-personal and/or institutional
- Termination of employment
- Termination of contract

b. SUBJECT (VOLUNTEER/PATIENT) RIGHTS

Every person has the right to:

- Consent or refuse collection, use or disclosure of their personal health information. Refusal is subject to legal exceptions. Example: a warrant or subpoena.
- Access their personal health information at any time.
- Request changes to any information that they feel is inaccurate or incorrect.
- Know who accesses when they access and uses their personal health information. A person can request an audit to be performed by the facility.
- Challenge the facilities in compliance with the Privacy Laws.

c. MAINTAINING CONFIDENTIALITY

- It is the responsibility of the researcher and/or health care provider to keep all subject, volunteer, patient, and employee information (personal or health) in the highest confidence.

- Privacy laws **DO NOT** affect mandatory reporting by regulated health care professionals for certain entities. Example: reportable diseases, child abuse etc.

Procedure:

1. Protect information that you have in your control: filing, locking cupboards, cabinets, log off secure network application when finished.

2. Do not email confidential or sensitive information with any patient identifiers to sources outside of your work facility.

3. Discuss the intended use and sharing of the information with the individual and respect their wishes regarding the use of their info. You can share information with other health care workers who are involved with the patients' management unless the patient tells you otherwise.

4. Maintain the confidentiality of information about staff and affiliates the same as you would for patients. Respect a colleague's right to privacy.

5. Access only that information which is necessary for your work. Do not access your own information, or family and friends' charts. This may lead to disciplinary action.

6. Do not share your password. Log out of all systems when you are finished.

7. Dispose of confidential information in the appropriate manner i.e., shredding.

8. When sending interdepartmental mail, consider the sensitivity of this mail. If it is sensitive, send in a sealed envelope.

9. Maintain confidentiality by discussing information in a private setting where no one can hear your discussion. Discussion of confidential information should not occur in public places-café, elevators, hallways, waiting rooms, home, etc.

10. If you use a wireless device (e.g., laptop, or mobile phone) perform the following guidelines:
    - Password protect all programs
    - Keep information stored on this device to a minimum. Download/upload from hospitals virtual drives.
    - When possible, remove patient identifiers from information.
    - Do not leave your wireless devices unattended. Make sure it is always in a secure place.
    - Anonymize subject data, when entering information on the 3T GE MR750

d. RESEARCH INVOLVING HUMAN SUBJECTS, SAMPLES OR POPULATIONS

- All studies involving human research must be approved via the Human Research Ethics board. The PI is responsible for listing all students, technicians and other personnel that may be working with human subjects or samples. All personnel must be identified to the REB and listed with the project. If new individuals join the project partway, their names must be forwarded to the REB.

- All information concerning human subjects and samples that are used for research are subject to the Personal Health Information Patient Act or PHIPA. PHIPA lists several security regulations that must be followed. Everyone that this pertains to must read through the regulations governing protection of patient identity. This information can be found by accessing the UWO Research Office website and then linking from there to the Ethics website.

- The main concern is that patient/volunteer identity must be held secure in all cases. Any release of name, initials, birthdates, addresses in and form (stored data files, hard copies, oral presentations, even verbally) are major contraventions of this legislation and the individual releasing such information (even inadvertently) will be held accountable including the institution.

- For all researchers using human subjects (volunteers/patients) and human samples in this city derived from LHSC. The Lawson Research Institute assumes responsibility for maintaining patient confidentiality regarding human subjects and samples for Research purposes. Therefore, all investigators (PI's, students, Post Docs, and technicians) using human subjects and samples must be listed by the LHRI research ethics board. This includes investigators that are not members of LHRI.

- Any portable devices (laptops, mobile devices, USB keys, etc.) that might contain human subject identification information must be stored in a secure site and the information on those devices must be encrypted so that if lost, patient identification is not compromised.