SOP Title	Privacy and Confidentiality of Personal Information-Investigator
Number.Version	N107.003
Effective Date	02/24/2025

Approvals

Name and Title of Signatories	Signature	Date mm/dd/yyyy
Erika Basile Director, Research Ethics and Compliance	Erika Basile	Mar 3, 2025
Dr. Isha DeCoito Chair, Non-Medical Research Ethics Board	Isha DeCoito	Mar 3, 2025

1. PURPOSE

This Standard Operating Procedure (SOP) describes the procedure to ensure the integrity and confidentiality of data collected within the framework of a study and the privacy of study participants.

2. GENERAL POLICY STATEMENT

This SOP is applicable to all studies undertaken at The University of Western Ontario and its affiliate institutions and to those research personnel responsible for ensuring the security and confidentiality of data, and participant information.

3. RESPONSIBILITY

The Principal Investigator is responsible for ensuring that the confidentiality and privacy aspects of the study meet all of the applicable regulations.

Any or all parts of this procedure may be delegated to appropriately trained study team members, but remain the ultimate responsibility of the Sponsor-Investigator or Qualified Investigator (QI)/Investigator.

4. DEFINITIONS

See Glossary of Terms.

5. SPECIFIC POLICIES AND PROCEDURES.

5.1 General Principles

5.1.1 Information that is disclosed in the context of a professional or research relationship must be held confidential to the extent permissible within the applicable law. Confidential information may be written, verbal, electronic, photographic or stored in any other medium (i.e., tissue, diagnostic images).

5.1.2 Protection of privacy and/or confidentiality in the context of research includes prevention of disclosure, to other than authorized individuals, of any information which could identify a research participant, or any Sponsor's proprietary information.

5.1.3 Every authorized person with direct access to data must comply with the regulatory requirements (e.g., Declaration of Helsinki, the directives of the ICH-GCP, etc.) and applicable privacy legislation for the maintenance of confidentiality, participant identity and respect for the proprietary information of the Sponsor or the Sponsor-Investigator.

5.1.4 Authentication of the person who has access to the data constitutes the most important aspect of security. It determines the overall level of protection and is linked to key elements of data security.

5.2 **Data Security**

5.2.1 Establish a mechanism for control of access to secure premises. Document the procedure. It is recommended that the control mechanism includes use of magnetic cards or a biometric recognition system that allows tracking of movement in and out of the premises, if applicable.

5.2.2 Retain a tracking document with the signatures and initials of all persons authorized to register data, or to make corrections to the study documents, with the essential study documentation.

5.2.3 Physical security concerns the premises where study files containing essential documents as well as computer equipment used for data management, such as telecommunication servers, database servers and computers are located. These rooms should be located in an area protected from possible disasters (e.g., water or fire damage, etc.), and be protected by a secure access control system.

5.2.4 Logical security concerns management of access to data, which includes identification, authentication, and authorization. In order to ensure logical security, the following measurements should be applied:

- Limit authorized access to members of the research team, and those identified by the protocol, the consent form, and the delegation of authority form;
- Grant privileges for physical or electronic access to data to personnel according to the roles and responsibilities defined by the Sponsor-Investigator or Qualified Investigator (QI)/Investigator.

5.2.5 Sponsor or Sponsor-Investigator: designate person in charge of system management (system administrator).

5.2.6 System Administrator's responsibilities include:

- Develop and enforce standardized procedures for logical security;
- Assign a different identification code to each user of the data management system;
- Ensure that users change their confidential password regularly, according to the period defined by the system administrator;
- Ensure the confidentiality of the authentication of system users, and document access tracking;
- Establish a Disaster Recovery Plan, for saving and recovering data, in the event of loss or disaster;
- Suspend the authorized access of a user after a given number of errors. Inform other users of this suspension. Update the delegation of tasks form, accordingly. Retrain user, if required. Document training; and
- Cancel access for research team members who leave the study (resignation, illness, parental leave, etc.). Update the delegation of tasks form, accordingly.

5.3 **Data Confidentiality**

5.3.1 A participant who authorizes access to their data must be reasonably assured that the Sponsor or Sponsor-Investigator, QI/Investigator, their authorized representatives, Research Ethics Board (REB), and regulatory inspectors of the regulatory authorities will take precautions to ensure that verified and collected data remain confidential.

5.3.2 Include a description of the provisions and limits of confidentiality within the context of the research study, in the informed consent process and form, as follows:

- The letter of information must describe to the participant who will have access to their information and for what purposes (e.g., , Research Ethics Board (REB), research sponsors and personnel monitoring/auditing the research on their behalf);
- Information collected during the research study will not be shared by the researcher without the participant's free and informed consent;
- Information pertaining to the research participant must be recorded in research case report forms (CRFs), and any other study documents that will leave the research site, including electronically captured data, in such a way as to protect participant identity. Participants will be identified with a unique identifier;
- No study materials sent to and/or retained by the sponsor will contain any identifying information. This includes, but is not limited to, investigational drug returns, test results, medical histories, and adverse event reports;
- Participant enrolment lists, copies of prescriptions and informed consent forms, which include identifying information, will be retained at the site. All research documents with participant identifiers should be kept separate from all study documents;
- Any reimbursements or stipends paid to the participants will be paid from the research account specific to the study, and not directly from the sponsor. This will ensure sponsor does not have access to participant names; and
- The Non-Medical Research Ethics Board (NMREB) review process governs the secondary use of the information gathered (for purposes other than the original intent), in accordance with the applicable regulatory guidelines.

6. REFERENCES

6.1. Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, December 2010.

6.2. Department of Justice (Canada), Personal Information Protection and Electronic Documents Act (PIPEDA), updated 2006.

6.3. US Department of Health and Human Services, Code of Federal Regulations, Title 45, Part 46, Protection of Human Subjects (45CFR46).

7. SOP HISTORY

SOP Number.Version	Key Changes	Effective Date mm/dd/yyyy
N107.001	Original	12/07/2015
N107.002	Update to NMREB Chair & Administrative Corrections	08/14/2018
N107.003	Update to NMREB Chair & Administrative Corrections	02/24/2025