

Title	Use and Disclosure of Personal Information
SOP Code	107.005
Effective Date	14-Apr-2026

Site Approvals

Name and Title (typed or printed)	Signature	Date dd/Mon/yyyy

1.0 PURPOSE

This standard operating procedure (SOP) describes the responsibilities of the Research Ethics Board (REB) and the REB office in protecting Personal Information (PI), including Personal Health Information (PHI), in accordance with applicable privacy legislation.

2.0 SCOPE

This SOP pertains to REBs reviewing research involving human Participants, particularly where identifiable PI or PHI is collected, used, disclosed, linked, or stored.

3.0 RESPONSIBILITIES

All REB members, REB Office Personnel, and Researchers are responsible for ensuring that the requirements of this SOP are met.

The Researcher is responsible for submitting information to the REB and to the Participant regarding the nature of the PI (including PHI) that will be collected for the research, including the manner in which it is identified, collected, accessed, used, disclosed, retained, disposed of, and protected.

The REB and the REB Office personnel are responsible for ensuring compliance with the applicable policies and procedures regarding the use and disclosure of PI. This includes evaluating privacy risk, reviewing data protection practices, and responding to potential or actual breaches of privacy.

Each organization's privacy office is responsible for providing Researchers and research staff with guidance on privacy policies and regulations.

4.0 DEFINITIONS

See Glossary of Terms.

5.0 PROCEDURE

Privacy is a fundamental value essential for the protection and promotion of human dignity. Breaches of privacy and confidentiality may cause harm to individuals or groups of individuals. Hence, PI must be collected, used, and disclosed in a manner that respects a research Participant's right to privacy, and in accordance with applicable federal and provincial privacy regulations.

Privacy regulations permit the use and limited disclosure of PI for research purposes, provided certain requirements are met. One of the key ethical challenges for the health research community is appropriately protecting the privacy and confidentiality of PI used for research purposes. The REB plays an important role in balancing the need for research with the risk of infringement of privacy, and in minimizing invasions of privacy for research Participants. Individuals must be protected from any harm that may result from the unauthorized use of their PI, and they should expect that their rights to privacy and confidentiality will be respected.

5.1 REB Review of Privacy Concerns

5.1.1 The REB shall review the submitted research to determine whether the Researcher has access to and/or is using PI, and whether appropriate privacy legislation is being followed;

5.1.2 In reviewing the research, the REB will include such privacy considerations as:

- The type of PI to be collected,
- The research objectives and justification for the requested personal data needed to fulfill these objectives,
- The purpose for which the personal data will be used,
- How the personal data will be controlled, accessed, disclosed, and de-identified,
- Limits on the use, disclosure, and retention of the personal data,
- Any anticipated secondary uses of identifiable data from the research,
- Any anticipated linkage of personal data gathered in the research with other data about research Participants, whether those data are contained in public or in personal records,

- Whether consent is required for access to, or the collection of personal data from Participants,
- How consent is managed and documented,
- If and how prospective research Participants will be informed of the research,
- How prospective research Participants will be recruited,
- The administrative, technical, and physical safeguards and practices in place to protect personal data including de-identification strategies and managed linkages to identifiable data,
- How accountability and transparency in the management of personal data will be ensured,
- Whether data will be stored or transferred across provincial or international borders and if so, how jurisdictional privacy laws will be met;

5.1.3 The REB must find that there are adequate provisions to protect the privacy interests of Participants before approving the research.

5.2 Receipt, Use, and Disclosure of PI

5.2.1 The REB Chair, REB members, and REB Office Personnel are bound by confidentiality agreements signed prior to the commencement of their duties;

5.2.2 The REB does not intentionally collect PI;

5.2.3 Subject to consent, as applicable, the REB is permitted to access PI for the purposes of review, approval, ongoing monitoring, and/or the auditing of the conduct of the research;

5.2.4 The REB office must adopt reasonable safeguards and ensure that training is provided for REB Office Personnel to protect PI from unauthorized access;

5.2.5 REB members or REB Office Personnel may consult with the REB Chair or Designee if they are uncertain about the appropriate use or disclosure of PI;

5.2.6 If any PI is received inadvertently in the REB office (e.g., disclosed by a Researcher), appropriate notification must take place and any corrective action that is required including the notification to the appropriate Organizational Official, must be undertaken. The facts surrounding any actual or suspected breach, the appropriate steps taken to manage the breach, remedial activities to address the breach, and the outcome must be documented. The PI must be destroyed in a secure manner in accordance with the organizational policies and procedures;

If there is an internal breach involving the use or dissemination of PI, the REB Chair or Designee will be notified, and if applicable, the appropriate

Organizational Official will also be notified, and a determination will be made in a timely manner regarding a corrective action plan. This process may include notification, containment, investigation, remediation, and strategies for prevention. The facts surrounding the breach or suspected breach must be documented. Documentation shall follow institutional privacy breach protocols and include audit trails, if available. The PI will be destroyed in a secure manner in accordance with the organizational policies and procedures;

5.2.7 At the discretion of the REB Chair or Designee, in consultation with the organization, the provincial privacy office (or equivalent) may be notified.

6.0 REFERENCES

See References.

7.0 REVISION HISTORY

SOP Code	Effective Date	Summary of Changes
SOP107.001	15-Sept-2014	Original version
SOP107.002	08-Mar-2016	No revisions needed
SOP107.003	08-Oct-2019	No revisions needed
SOP107.004	15-May-2023	No revisions needed
SOP107.005	14-Apr-2026	<p>1.0: revised 'duties' to 'responsibilities; added 'including Personal Health Information (PHI), in accordance with applicable privacy legislation.'</p> <p>2.0: revised from 'This SOP pertains to REBs that review human participant research in compliance with applicable regulations and guidelines; changed 'guidelines' to 'policies'; added reference to PHI.</p> <p>3.0: added 'The REB and the REB Office personnel are responsible for ensuring compliance with the applicable policies and procedures regarding the use and disclosure of PI. This includes evaluating privacy risk, reviewing data protection practices, and responding to potential or actual breaches of privacy.'</p> <p>5.0: minor wording changes, e.g. 'provided' in place of 'as long as; 'must' in place of 'should'; 'with' in place of 'against'; 'will be' in place of 'are'.</p> <p>5.1.2: added 'Whether data will be stored or' transferred across provincial or international borders and if so, how jurisdictional privacy laws will be met';</p> <p>5.2.6: added '...any actual or suspected breach...'; revised 'as per' to 'in accordance with'.</p>

		5.2.7; revised 'notification of the appropriate Organizational Official' to "the appropriate Organizational Official will also be notified.'; 3 rd sentence, added 'and appropriate steps taken to manage the breach and the outcome will be documented. Documentation shall follow institutional privacy breach protocols and include audit trails, if available.'; revised 'as per' to 'in accordance with'.