

<b>Title</b>	<b>Document Management</b>
<b>SOP Code</b>	303.005
<b>Effective Date</b>	14-Apr-2026

### Site Approvals

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

## 1.0 PURPOSE

This standard operating procedure (SOP) describes the requirements for document management, including document retention and document archiving. This SOP applies to documents submitted to the Research Ethics Board (REB) for initial or for continuing review, as well as to all REB administrative documents, including those stored in electronic and cloud-based platforms.

## 2.0 SCOPE

This SOP pertains to REBs that review human Participant research in compliance with applicable regulations and policies.

## 3.0 RESPONSIBILITIES

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

This includes the institutional responsibility to ensure that systems used for document management (including cloud-based or software-as-a-service [SaaS] platforms) comply with security, confidentiality, and integrity standards applicable under Canadian and international guidance.

## **4.0 DEFINITIONS**

See Glossary of Terms.

## **5.0 PROCEDURE**

The REB office must retain all relevant records (e.g., documents reviewed and approved or disapproved, REB meeting minutes, correspondence with Researchers, written SOPs, and REB membership rosters) to provide a complete history of all actions related to the REB review and approval of submitted research. Such records must be retained for the length of time required by applicable regulations and guidelines.

Relevant records must be made accessible to authorized regulatory authorities, representatives of the organizations, Researchers, and funding agencies within a reasonable time upon request.

### **5.1 Research-Related Documents**

5.1.1 The REB office retains the submission materials for all research that have been submitted for REB review and have been either approved, acknowledged, or disapproved;

5.1.2 Research-related documents include, but are not limited to, the following (as applicable):

- REB initial application form and all associated attachments;
- Correspondence between the REB and the Researcher, including REB approval letters, requests for modifications, etc.;
- Records of ongoing review activities such as,
  - Reportable event submissions, including reports of significant new findings, Data and Safety Monitoring Board (DSMB) reports, interim analysis reports, local adverse events, research deviations, privacy breaches, any investigations into allegations of serious or continuing non-compliance, and reports of inspections and audits by regulatory agencies or others,
  - Modifications to the application package including amendments to the research protocol and any other documents associated with the conduct of the study within the scope of REB review and approval;
- All other continuing review applications and documents associated with that review;
- Copies of correspondence between the REB and regulatory agencies;
- Reports of any complaints received by the REB and their resolution.

## **5.2 REB Administrative Documents**

5.2.1 The REB office retains all administrative records related to the REB review activities;

5.2.2 REB administrative documents include, but are not limited to, the following:

- Agendas and minutes of all REB meetings;
- Submitted REB member reviews;
- REB member records:
  - Current and obsolete REB membership rosters, including alternate REB members,
  - CVs and training/qualification documentation of current and past REB members;
- Signed conflict of interest and confidentiality agreements;
- Current and obsolete SOPs;
- Current and obsolete documentation of the REB Chair or Designee's delegation of authority, responsibilities, or specific functions;
- Records of registration of the REB with the US Office of Human Research Protection, if applicable, and REB membership updates.

## **5.3 Document Access, Storage, and Archiving**

5.3.1 Access to individual research projects and related documents is role-based to ensure that users only have access to documents and activities that are required by their role;

5.3.2 The REB records are housed securely with back-up, disaster, and recovery systems in place.

## **5.4 Confidentiality and Document Destruction**

5.4.1 All submissions received by the REB are considered confidential and are accessible only to REB members (including the REB Chair and Vice-Chair), and the REB Office Personnel;

5.4.2 Relevant research projects and associated documents may be made accessible to members of regulatory agencies, or representatives of the Sponsor or Researcher for review. Access is limited to the applicable research and research-related submissions; REB records may be accessed by authorized institutional officials for audit, accreditation, or quality purposes. These records are not shared directly with Sponsors or service providers unless required by law or institutional policy.

- 5.4.3 The REB will retain required records (e.g., research-related or REB administrative documents, as applicable) for a minimum of 3 years after completion/termination of the trial, or for the maximum amount of time stipulated in any applicable governing regulation(s);
- 5.4.4 Any confidential materials in paper format in excess of the required documentation will be shredded.

## **5.5 Use of Electronic and Cloud-Based Application and Document Management Systems**

- 5.5.1 Institutions are responsible for ensuring that any electronic or cloud-based systems used to create, store, manage, or archive REB records are fit for purpose and support the integrity, confidentiality, reliability, and accessibility of those records throughout their lifecycle;
- 5.5.2 Systems used for REB document management must be implemented and maintained in a manner consistent with applicable regulatory, ethical, and privacy requirements, including, where applicable, US FDA 21 CFR Part 11 (Electronic Records and Electronic Signatures), federal and provincial privacy legislation, and institutional information security policies;
- 5.5.3 Electronic systems must support the accuracy, completeness, and retrievability of REB records such that a complete history of REB review, decision-making, approvals, amendments, and archival actions can be reconstructed and made available for inspection, audit, or regulatory review as required;
- 5.5.4 Institutions must ensure that access to electronic REB systems is controlled and appropriate to users' roles and responsibilities, and that responsibilities for system administration, oversight, and record management are clearly defined;
- 5.5.5 Where audit trails or system logs are used, they must be retained and made available in accordance with applicable regulatory and institutional requirements;
- 5.5.6 Where REB records are stored or processed using cloud-based services, institutions are responsible for ensuring that data handling practices comply with applicable jurisdictional privacy requirements and that arrangements are in place to protect confidentiality, security, and regulatory access;
- 5.5.7 Institutions must have processes to ensure the continuity, retention, and accessibility of REB records in the event of system upgrades, migrations, vendor changes, or system decommissioning.

## **6.0 REFERENCES**

See References.

## 7.0 REVISION HISTORY

SOP Code	Effective Date	Summary of Changes
SOP303.001	15-Sept-2014	Original version
SOP303.002	08-Mar-2016	5.3.2: revised to state securely housed with removal of the reference to an onsite location.
SOP303.003	08-Mar-2019	5.1.2: deletion of 'signed' from first bullet; 5.3.1: deletion of 'and to centre and Researcher profiles'; 5.4.1: deletion of 'as well as to organizational official(s)'; 5.4.2: deletion of 'other' and 'guest'
SOP303.004	15-May-2023	5.4.4: remove specific reference to HC retention requirement
SOP303.005	14-Apr-2026	<p>1.0: added 'including those stored in electronic and cloud-based platforms' to the last sentence.</p> <p>3.0: added 'This includes the institutional responsibility to ensure that systems used for document management (including cloud-based or software-as-a-service [SaaS] platforms) comply with security, confidentiality, and integrity standards applicable under Canadian and international guidance.'</p> <p>5.1.2: revised bullet point 3, sub-bullet 2, from 'Modifications to the application including amendments to the research and/or any changes to the consent(s), participant materials or Investigator Brochures' to indicate 'application <i>package</i>' and to clarify 'any other documents associated with the conduct of the study within the scope of REB review and approval.'</p> <p>5.1.2: bullet point 4 revised to '<i>All other continuing review applications and documents associated with that review</i>'.</p> <p>5.5 : New section to align SOP 303 with current international and national standards for document management in research ethics oversight: ICH E6(R3) 2025: Computerised systems and TCPS2 (2022): Chapter 5, Privacy and Confidentiality</p>