fraserhealth
Better health. Best in health care.

GUIDANCE NOTES ON RETENTION AND DISPOSAL OF RESEARCH DATA

INTRODUCTION

Researchers are responsible for implementing appropriate privacy protections to safeguard information collected about study participants throughout the entire lifecycle of the research, including after the information is collected and analyzed. This guidance note describes standards and expectations for the retention, disposal, and destruction of research data.

GUIDANCE NOTE #1: DEFINITIONS

The TCPS 2 provides the following definitions:

Retention: Retention refers to the specified period during which research data and records must be kept and maintained. This period is determined by ethical, legal, and institutional requirements to ensure data integrity and compliance, and that data is available for verification, replication, and future research purposes.

Destruction: Destruction involves the complete and irreversible elimination of data and records. This process ensures that the data cannot be reconstructed or retrieved, thereby protecting the privacy and confidentiality of research participants.

Disposal: Disposal is the process of discarding research data and records that are no longer needed at the end of the specified period. This process must be conducted in a manner that ensures the data is securely and permanently removed, preventing unauthorized access or misuse.

Open Access Repository: An Open Access Repository is a digital platform that provides free and unrestricted access to research data and publications. These repositories promote transparency, reproducibility, and collaboration by making research outputs widely available to the public and the scientific community.

Data and Records: All documents and information collected, used, or stored during research involving health research. This includes primary data collection (e.g., surveys, interviews) and secondary use of data (e.g., health care records, biological specimens).

> **Directly identifying information:** The information identifies a specific individual through direct identifiers (e.g., name, social insurance number, personal health number).
>
> **Indirectly identifying information:** The information can reasonably be expected to identify an individual through a combination of indirect identifiers (e.g., date of birth, place of residence or unique personal characteristic).
>
> **Coded information:** Direct identifiers are removed from the information and replaced with a code. Depending on access to the code, it may be possible to re-identify specific participants (e.g., the principal investigator retains a list that links the participants' code names with their actual names so data can be re-linked if necessary).

Anonymized information: The information is irrevocably stripped of direct identifiers, a code is not kept to allow future re-linkage, and risk of reidentification of individuals from remaining indirect identifiers is low or very low.

Anonymous information: The information never had identifiers associated with it (e.g., anonymous surveys) and risk of identification of individuals is low or very low.

GUIDANCE NOTE #2: ETHICAL CONDISERATIONS FOR DATA RETENTION AND DISPOSAL

The Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2) requires researchers to assess privacy risks and threats to the security of information for all stages of the research life cycle, including the retention and disposal of data following the completion of a research project, and to implement appropriate measures to protect information.

Ensuring the privacy and confidentiality of research participants requires an appropriate, thoughtful plan for how research records, including data, will be retained and disposed of following the study completion. Data should only be retained for as long as necessary to fulfill the purpose for which it was collected. Retaining data beyond this period without a valid reason can lead to privacy concerns and potential misuse. When data is no longer needed, it must be disposed of securely to prevent unauthorized access, disclosure, or misuse.

It is vital researchers develop appropriate plans for all information collected about the participants beyond the final data set, and communicate this to the REB. For instance, studies using semi-structured interviews should provide details to the REB of how the information in all formats, such as audio recordings, interview notes, transcripts, and final coded data, will be retained and disposed of. For studies and trials in which data and/or biological specimens will be sent to a sponsor or third-party site, the retention and disposal plans at all sites must be detailed in the REB application. All researchers have an ethical responsibility to protect individuals' privacy and confidentiality throughout the data lifecycle, including during disposal.

GUIDANCE NOTE #3: RETENTION REQUIREMENTS

In accordance with TCPS 2, the Fraser Health Research Ethics Board (FHREB) does not mandate a specific data retention and destruction period for research records. It is the responsibility of the research to comply with all applicable policies, regulations, and requirements regarding data retention. The Fraser Health Research Policy requires research records, including study data, be retained for a minimum of 5 years following study completion (i.e. after all data collection is complete and a study close-out has been issued by the REB) in order to protect the integrity of the research. Clinical trials regulated by Health Canada are required to retain research records for 15 years. Health Canada reduced the retention period for regulated trial records from 25 years effective February 11, 2022 (more information).

There are many factors to consider with respect to the appropriate data retention period, including:

1) Regulatory requirements
2) Data access agreement (DAA) requirements
3) Funder/sponsor requirements
4) Disciplinary standards
5) Formal data sharing agreements
6) Necessary requirements to fulfill the research purpose

The researcher is responsible for ensuring appropriate safeguards for the security of the data during the retention period. The plans for all of the site data following study completion must be submitted to the FHREB for review as part of the initial Ethics application and the study close out notification. Additionally, the data plans for all of the extracted Fraser Health system data must be submitted to the Fraser Health Information Privacy team in the Data Access Agreement (DAA). This includes:

1) Where the study data will be stored
2) Who will have access to the data
3) The security protections for the data
4) Any planned secondary use of the data
5) When and how data will be destroyed

In certain cases where identifiable data has been collected, such as with audio and video recordings, it may be appropriate to destroy the data immediately following transcription to ensure protection of participant confidentiality. The DAA will assist in identifying a finalized process to mitigate risk and ensure that data retention is defined by research purpose and elimination is thorough.

GUIDANCE NOTE #4: DISPOSAL OF DATA

Researchers must describe the data disposal mechanisms for all forms of research data and personal information in their submission to the FHREB and the timelines for such disposal. This includes hard-copy documents (e.g. signed consent forms and paper-based data collection forms), digital data (e.g. eCRFs, master tracking logs, DICOM images), as well as audio and visual media stored on electronic devices such as audio and video recorders, tablets, USB keys, etc. The mechanisms for data disposal must be appropriate for the medium and be irreversible.

Any of the following are acceptable methods of data destruction:

- Using a software utility that erases by overwriting or encrypting the data;
- Magnetically erasing (degaussing) the data;
- Formatting a device after encryption it.
    - For low-risk information formatting a device to include full disk, device-level, and media-level encryption.
    - For med-high risk information formatting file-level encryption or transparent database engine encryption;
    - The British Columbia Information and Privacy Commissioner in their interpretation of the BC Freedom of Information and Protection of Privacy Act (FIPPA) enacts a legal requirement to encrypt Personal Information stored on devices.
    - International travel may require devices to be unencrypted or hand over encryption keys, therefore all encrypted devices should not travel abroad.
    - An analysis of appropriate Encryption requirements is best performed during a Privacy Impact Assessment (PIA) or a Security Threat Risk Assessment (STRA).
- Using a machine that physically deforms or destroys the device to prevent the data from being recovered.
- Using the ”Empty Recycle Bin/Trash”, ”Delete”, ”Remove”, and ”Format” operating system commands do not destroy data and therefore are not acceptable methods for preparing media for transfer or disposal.
- Data destruction methods must comply with the minimum standards set out in the IT Media Sanitization (ITSP.40.006) publication issued by the Government of Canada.

Paper-based records: Paper records should be destroyed by cross-shredding, incineration, or similar methods that do not allow for retrieval or re-identification.

Digital data: It is not sufficient to use the “Delete”, “Remove”, “Empty Recycle Bin/Trash” commands to dispose of digital data. Digital data should be removed using methods that permanently destroy or render the data irrecoverable, such as overwriting, degaussing (magnetically erasing) the data, or physically destroying the media.

GUIDANCE NOTE #5: OPEN ACCESS REPOSITORIES

Researchers who intend to deposit their data in an open access repository must disclose this intention in the REB application and in the consent process. While the sharing of data via open access repositories may provide benefits, including the reduction of burden on participants, it may also create additional privacy risks. Researchers are responsible for providing an appropriate justification to the REB and for ensuring compliance with all applicable regulatory, legal, and policy requirements.

In order to deposit data in an open access repository, informed consent from the participant is required. The consent form must include the following information:

1. A description of what open access is and what it means for the research participant, including:
    - Who will have access to the data,
    - How will the data be used,
    - In what format the data will be deposited and whether identifiers will be removed,
2. A clear statement that the data will be publicly available,
3. A clear statement that once data are made publicly available, the participant will no longer be able to withdraw their data,
4. A clear statement, where applicable, that making data publicly available has the potential for increasing participant risk.

For studies that did not seek prior consent for the deposit of data in an open access repository, researchers should consult the Panel of Research Ethics' Guidance on Depositing Existing Data in Public Repositories.