Research Ethics Board

REB Guidance and Information Document

SOP File #	**REB.INFO.503**
Title	**Sensitive Data**
Effective Date	June 2022
Next Review	2027
Next Administrative Review	2025

1. Purpose

One of the guiding principles of the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS) is concern for welfare. Contributing factors to welfare are privacy and control of information about an individual and the treatment of human biological materials according to the desires of the person from whom the information or materials were collected. Researchers must have in place procedures for the protection of identifiable, sensitive and/or confidential information obtained or collected during participation in a research study or for use in a research study. Identifiable information is any information that may reasonably be expected to identify an individual, alone or in combination with other available information.

2. Definitions

See the MSVU REB **Glossary of Terms (REB.INFO.001)**
See the glossary of terms related to sensitive data and the **Sensitive Data Toolkit** from the Digital Research Alliance of Canada/Sensitive Data Experts - Training Resources | Digital Research Alliance of Canada (alliancecan.ca)

3. Notice to Researchers

The information in this document is for information and guidance purposes only. Each research study poses unique properties and/or situations that may require additional or different guidance than what is presented in this document. The information in this document is meant to provide general situational advice and does not constitute research ethics compliance in absolute form. If you have any questions, please contact ethics@msvu.ca .

4. Background

The term "sensitive data", for the purposes of this guidance document includes any data that, if released to the public, would have an adverse effect or cause potential harm to the research participant or community. Sensitive data can be contextual. The underlying assumptions tend to be that the information being requested may evoke a strong emotional response, and it may be threatening or even damaging to the individual to share such information. Researchers should consider if the requested information or the disclosure of information could potentially harm participants and/or be something they prefer not to share with wider society? A researcher also needs to consider whether the sharing of that information may have an impact beyond the person providing the information. Could the disclosure of the information potentially harm

other individuals such as family members or the community to which the person belongs? It is important that researchers think critically about the impact from the collection and use of data on the participants or community groups associated with the project. Researchers may be assessing sensitive information, the publication or analysis of which may have direct impact on agencies, communities or individuals. For example, collection and use of archive, historical, legal, online or visual materials may raise ethical issues (e.g., for families and friends of people deceased). In particular, consideration of risks to the research participants versus benefits needs to be weighed by researchers.

4.1. The U.S. Office of Human Research Protections (OHRP) provides the following list of categories of information that could be considered sensitive.
- Information relating to sexual attitudes, preferences, or practices;
- Information relating to the use of alcohol, drugs or other addictive products;
- Information pertaining to illegal conduct;
- Information that if released could reasonably be damaging to individuals' financial standing, employability, or reputation within the community;
- Information that would normally be recorded in a patient's medical or health record, and the disclosure of which could reasonably lead to social stigmatization or discrimination;
- Information pertaining to an individual's psychological well-being or mental health;
- Genetic information - DNA and RNA analysis, chromosomal information.

4.2. Personal Identifiable Information (PII) is any piece of information that may be reasonably expected to identify an individual, alone or in combination with other available information. Individual personal data may include:
- Name, address, telephone, email (personal not business)
- Race, ethnic origin or religious political beliefs or associations
- Age, sex, sexual orientation, marital status or family status
- Identifying number (Student ID, SIN, etc.)
- Fingerprints, blood type, or inheritable characteristics
- Medical or personal history, including diagnosis, opinions, collected via various electronic apps (e.g., fitness apps_.
- Education, employment, financial, or criminal history
- Classified information,
- Biometric data such as: facial features/recognition, voice recognition, fingerprints, etc.

4.3. It is important to note that these lists are not exhaustive and depending on the type of information that is being elicited and the context within which data collection occurs, information may or may not be considered sensitive.

4.4. The identification of information as sensitive does not preclude a researcher from including such data in a study. The collection of sensitive data may increase the level of risk to participants, but this does not mean the conduct of study cannot be justified.

4.5. In reviewing any study which includes sensitive data, the REB as well as the researcher, needs to consider the magnitude or seriousness of the risk to participants and the probability of potential harm in relation to the potential benefits of the research. In addition, the researcher should consider means to eliminate or mitigate the risk to participants.

5. Guidance/Information/Procedures

5.1. Protecting Identifiable Research Data

5.1.1. The level of data security necessary is relative to the risk posed to the participant should be personally identifiable information be inadvertently disclosed or released as a result of malfeasance.

5.1.2. Data sets with direct identifiers and identity-only data sets shall always be stored in a secure location and in secure data-encrypted form.

5.1.3. For data that retains identifiers, investigators must consider adequate administrative, physical, and technical safeguards.

5.1.4. When a study involves greater than minimal risk, researchers are encouraged to consult with appropriate information technology and security experts.

5.1.5. Tips for researchers include:

- Collect the minimum identifying data required.
- De-identify data as soon as possible after collection and/or separate data elements into a coded data set and an identity-only data set.
- Destroy raw identifying data as soon as possible and in accordance with the data retention policies or requirements.
- Treat data that cannot be reasonably de-identified as personally identifiable data.
- Use secure data encryption if identifiable information is: (1) stored on a networked computer or device, (2) stored on or transmitted via the web, (3) stored on a device which is not permanently located in a secure location.
- Limit access to personally identifiable information.
- When identifiable information is stored in personal or university-owned or -maintained computer, researchers are strongly encouraged to ensure that this computer is professionally administered and managed by the institution's Information and Technology Services or equivalent department.

5.2. Electronic Data

5.2.1. When collecting data online, researchers should be cautious of stored IP addresses and data that could be accessed by a third party. Researchers should make sure to encrypt identifiable data before it is transferred over a network or over email.

5.2.2. When using an online data collection site, researchers should carefully review the site's data security policy.

5.2.3. A dataset may be stored online (e.g., on a cloud storage system) only if it does not contain identifiable information or has first been encrypted so that, should there be a security breach, the data cannot be linked back to individual participants.

5.2.4. If considering storing data on a cloud or platform outside of the institution, researchers should first consult their institution's technology experts to determine which cloud computing service to use.

5.2.4.1. Important considerations include data storage location; backup policy; deletion policy; rights that the cloud provider claims for the data; isolation guarantees that the provider offers. Researchers may wish to consider using local hosting options.

5.2.5. Use caution when utilizing involving third-party sites. These sites may store data on backups or server logs beyond the time frame of the research and their security measures may not match those of investigators.

5.3. International Research

5.3.1. Researchers need to make sure that they have appropriate security measures in place while in the field, while in transit, and back at their home institution.
5.3.2. Depending on a number of factors, including political climate and availability of secure storage locations, researchers may find it difficult to maintain data security while in the field.
5.3.3. When travelling across international borders, researchers should be aware that governments can and will, at their discretion, take an electronic device, search through all the files, and may keep it for further scrutiny.

5.4. Data Transmission

The transfer of data via e-mail is not secure. Researchers should consider:

- Encrypt data before transmitting, or
- Ensure the transmission channel is encrypted
- In either case, the encryption key(s) must be stored separately from the data

5.5. Data Storage

5.5.1. Federal Regulations require research records to be retained for at least 3 years after the completion of the research and MSVU regulations require that data are kept for at least 5 years.
5.5.2. Another good practice is to retain data until there is no reasonable possibility that you will be required to defend against an allegation of scientific misconduct.
5.5.3. These regulations do not specify when you must destroy data, they only state the minimum amount of time you must retain it.
5.5.4. Ideally, all researchers should clearly define the data retention/destruction/sharing/deposit requirements in the consent form, so that participants can be fully informed in the consent process.
5.5.5. If researchers wish to reuse data for subsequent studies, researchers should clearly state in your consent form that data may be retained for use in future studies. In these cases, researchers should, if possible, destroy any identifying information and linking files once you have kept them for the longest applicable period.

6. Acknowledgements

The development of this document has benefited directly from similar documents made public by the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (TCPS). In some instances, specific formulations drawn from these sources have been incorporated into this document. Specific iterations were drawn from the following:

- Canadian Institutes of Health Research - CIHR Best Practices for Protecting Privacy in Health Research (September 2005) - CIHR (cihr-irsc.gc.ca) – Retrieved February 2022
- Vancouver Island University - Data Retention and Destruction | Research Ethics Board | Vancouver Island University | Canada (viu.ca) – retrieved January 2022
- University of Toronto - Sensitive Data | University of Toronto Libraries (utoronto.ca) – retrieved March 2022
- University of Waterloo - Guideline for researchers on securing research participants' data | Research | University of Waterloo (uwaterloo.ca) – retrieved November 2021
- Panel on Research Ethics - Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2018) – Chapter 5: Privacy and Confidentiality (ethics.gc.ca) November 2021

- Office for Human Research Protections – Certificates of Confidentiality - Privacy Protection for Research Subjects: OHRP Guidance (2003) | HHS.gov - retrieved November 2021.
- Digital Research Alliance of Canada – Sensitive Data Toolkit – Retrieved May 2022
    - *Sensitive Data Toolkit for Researchers Part 1: Glossary of Terms for Sensitive Data used for Research Purposes | Zenodo*
    - Sensitive Data Toolkit for Researchers Part 2: Human Participant Research Data Risk Matrix | Zenodo
    - Sensitive Data Toolkit for Researchers Part 3: Research Data Management Language for Informed Consent | Zenodo

7. Modification History

INFO Number & Version	Key Changes	Effective Date
REB.INFO.503	Revised to a guidance document, formerly SOP.127. Updated to reflect current requirements and practices and revised for clarity	June 2022
REB.SOP.127	Original Version	January 2012

This Page is intentionally left blank.