Fraser Health Research Ethics Board
Department of Evaluation and Research Services , FHA
400 – 13450 102 Avenue, Surrey, BC V3T 0H1
Phone: (604) 587-4436 Fax: (604) 930-5425

GUIDANCE NOTES ON PRIVACY, CONFIDENTIALITY & DATA SECURITY

INTRODUCTION

Respect for privacy is a foundational principle of ethical research, codified in legislation as well as the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2). This guidance note describes the ethical duties of confidentiality and protection of privacy in research, the minimum standards for data security, and the submission requirements for review.

GUIDANCE NOTE #1: DEFINITIONS

The TCPS 2 provides the following definitions:

> **Privacy:** An individual's right to be free from intrusion or inference by others. This includes the right to control information about oneself. Privacy is respected if an individual has an opportunity to exercise control over personal information by consenting to, or withholding consent for, the collection, use and/or disclosure of information.
>
> **Confidentiality:** The ethical duty of confidentiality refers to the obligation of an individual or organization to safeguard entrusted information. The ethical duty of confidentiality includes obligations to protect information from unauthorized access, use, disclosure, modification, loss or theft. Fulfilling the ethical duty of confidentiality is essential to the trust relationship between researcher and participant, and to the integrity of the research project.
>
> **Security:** The measures used to protect and safeguard information.

GUIDANCE NOTE #2: REQUIREMENTS FOR SUBMISSION

Article 5.3 of the TCPS 2 states "Researchers shall provide details to the REB regarding their proposed measures for safeguarding information, for the full life cycle of information: its collection, use, dissemination, retention and/or disposal."

Submissions to the FHREB must include the following information in the protocol or supplementary documentation:

1. The types of information collected for the study and the source of collection
2. The purpose(s) for which information will be used, including any secondary uses
3. The proposed measure for safeguarding information at all stages of the research (e.g., collection, use, dissemination, retention, disposal)
4. Who will have access to the information/data (including translators and transcriptionists), and how they will be made aware of their duties of confidentiality
5. Risks to the participants should their data security be breached
6. The mechanisms for study data transfer (as applicable)

7. Any reasonably foreseeable disclosures of information
8. Any intentions to link the data with other data sources about the participants

2.1 Studies using data held or maintained by Fraser Health:

Studies that use personal and/or non-public information held or maintained by Fraser Health, such as medical records or administrative data, are required by the Fraser Health Office of Information Privacy to complete a Data Access Agreement. The Data Access Agreement application is appended to the Fraser Health Initial Application for Ethical Review (for harmonized studies submitted through the Provincial Research Ethics Platform, the Data Access Agreement application is in the Institutional Approval Form for Harmonized Studies). The FHREB Office will transfer the study file to the Privacy Office for the Data Access Agreement once the ethics approval is issued.

GUIDANCE NOTE #3: TYPES OF INFORMATION

Researchers must specify what specific information will be collected (e.g., tissue samples, medical record data, etc.), the form of the information (e.g., electronic, paper, audio recordings, etc.), as well as the level of identifiability of this information.

In determining the level of identifiability, researchers should consult the following definitions provided by the TCPS 2:

1. **Directly identifying information**: the information identifies a specific individual through direct identifiers (e.g., name, social insurance number, personal health number).
2. **Indirectly identifying information**: the information can reasonably be expected to identify an individual through a combination of direct identifiers (e.g., date of birth, place of residence or unique personal characteristic).
3. **Coded information**: direct identifiers are removed from the information and replaced with the code. This is sometimes referred to as “de-identified” information.
4. **Anonymized information**: the information is irrevocably stripped of direct identifiers, a code is not kept to allow future re-linkage, and the risk of re-identification of individuals from remaining indirect identifiers is low or very low.
5. **Anonymous information**: the information never had identifiers associated with it (e.g., anonymous surveys) and the risk of identification of individuals is low or very low.

While privacy risks decrease as the information becomes more difficult to associate with a specific individual, it is not always practicable or desirable to maximize the anonymity of the information collected. For instance, where data has been permanently stripped, the ability of participants to withdraw from the study or receive their results from a trial is not possible.

The FHREB expects that most information collected as part of a research study will be, at minimum, coded/de-identified where possible. Study codes should be made up of unique combinations of numbers and/or letters that are unrelated to the participant’s identity. The key

that links the participants' identities with study codes should be kept separate from the data in a secure, password-protected file.

In cases where the collection of personal identifiers are necessary for the feasibility and validity of a study, the researchers should provide a strong justification for this need. The consent form should also clearly state that information will be directly/indirectly identifiable, and that this is usual in most research studies.

3.1 Identifiers on source documents for clinical trials:

Source documents refer to the original documents, data, and records from which clinical research data is obtained. Source documents maintained by the researcher must not have direct identifiers. In cases where source documents include copies of original health records, these copies should be de-identified.

3.2 Laboratory reports and requisitions:

The standard of practices for Fraser Health Laboratory Services requires the use of a unique identifier for the research participant (e.g., name, PHN, MRN) for the automatic production of reference ranges for the particular lab value of interest. Fraser Health Laboratory Services will include the specified identifier on the lab report, which will also be available in the Meditech system.

GUIDANCE NOTE #4: ETHICAL DUTY OF CONFIDENTIALITY

When research information is collected with the promise of confidentiality, the duty to protect that information is paramount. Researchers are required safeguard information entrusted to them and not misuse or wrongfully disclose this information. The ethical duty of confidentiality applies regardless of whether the research data is directly collected from participants, or from secondary sources like medical records, and should be considered throughout all stages of the research, including the recruitment and consent processes, as well as after the study is completed.

This is ethical duty must be balanced in relation to other ethical considerations, including any legal or professional requirements to disclose information collected in the research context. For example, in certain exceptional situations, researchers may be required to report information shared confidentially by research participants to authorities for the purposes of protecting the life or safety of the party or a third party.

Researchers are expected to be aware of circumstances in which there is a reasonable likelihood that a disclosure of confidential research information may be required, including studies that:

1. Test for reportable diseases, such as HIV or Hepatitis C
2. Address issues of suicidality or self-harm
3. Address issues of harm to others, particularly children

Researchers are expected to consider such possible disclosures in the design of the research to avoid or mitigate such foreseeable conflicts. In cases where it is reasonably likelihood the research may be subject to court subpoenas or other legal challenges to the ethical duty of confidentiality, the researchers are strongly encouraged to seek legal counsel and consult with the Department of Evaluation and Research Services in advance of the ethics submission.

In certain circumstances, participants may specifically request to waive their confidentiality and have their contributions directly recognized. In these cases, researchers should accommodate these requests to the extent possible. Researchers should take care to obtain consent from such participants and negotiate the specifics of how such identification and/or recognition of contribution will occur. These requests, however, must take into consideration the potential for other participants or members of a group to be identified by another participant's desire to waive anonymity.

4.1 Breaches of privacy/confidentiality:

Breaches of privacy and confidentiality can have far-reaching consequences, such as potentially causing harm to the participant, the trust relationship between the researcher and the participant, other individuals and groups, and to the reputation of the research community.

In circumstances where personal information collected as part of a research project is inadvertently disclosed, the Principal Investigator must submit a Protocol Deviation Report to the FHREB within fifteen days of discovering the breach. Where the breach involves data under Fraser Health's custodianship or stewardship, such as information collected from medical records, the Principal Investigator is also responsible for reporting the breach directly to Fraser Health's Office of Information Privacy. The FHREB will work with the Privacy Office and the Principal Investigator to determine the most appropriate course of action and mitigation strategy.

4.2 Studies using audio-recording, video-recording, photography, or other recorded observations:

Extra precaution should be taken with recorded observations that may identify participants during the transportation and storage of this information. Where possible, information recorded on devices, such as audio-recorders, should be encrypted. Where this is not possible, additional physical safeguards, such as storing the recorders in locked briefcases, should be adopted. The details of who will have access to the photographs/recordings and the methods used to protect the participant's identity should be disclosed in the consent form. State how long the photographs/recordings will be maintained, where they will be stored and how they will be destroyed. If there are plans to use these materials for any other purpose than the research project described in the consent form, separate consent is required.

GUIDANCE NOTE #5: DATA SECURITY

Researchers are responsible for protecting their data at all stages of the research life cycle. While the FHREB expects that all data will be appropriately protected, extra protections may be required when data is collected with direct or indirect identifiers and/or where the data is of a particularly sensitive nature.

Safeguards for protecting research data may be:

1. **Physical**: Physical safeguards refer to the physical measures used to protect data, such as storing data in locked filing cabinets, and using locked briefcases to physical transport data.
2. **Administrative**: Administrative safeguards refer to organizational rules that limit the authorization and access to data. This can include limiting the amount of research team members who have access to data to a "need to know" basis, developing data security SOPs, and requiring all research team members to complete training in privacy and confidentiality standards.
3. **Technical**: Technical safeguards include measures such as password, firewalls, user identifications, and encryption that protect data from unauthorized access, loss, or modification.

Researchers should consider all applicable and appropriate safeguards for protecting their data security in their data management plan. At minimum, all research data should be kept in a secure locked location, and computer files should be encrypted and password protected. **The Fraser Health standard for encryption is 256 Bit.**

Fraser Health provides Fraser Health researchers with a number of institutional supports for protecting data, including access to secure M: drive folders, Sharepoint, and Cerberus Secure File Transfer.

GUIDANCE NOTE #6: DATA TRANSFER

Special precaution should be taken whenever personal information or data is transferred outside of the institution. The modalities through which data will be transferred and the security protections must be disclosed. Electronic modalities should, at minimum, be encrypted.

6.1 Data transfer outside of Canada:

Any transfer of personal information outside of Canada must be disclosed on the consent form. Participants must be made aware that laws regarding protection of privacy and information in other countries may not be as strict as in Canada. This includes transfer for transcription and/or translation purposes. The protocol and consent form must specify the locations where data will be sent, who will have access to the data, and the provisions to protect confidentiality.

GUIDANCE NOTE #7: DATA LINKAGE

If data will be linked to an external data source, the mechanism of the linkage must be detailed, including who will perform the linkage, what identifiers will be used to link the data, how the data will be subsequently stripped of identifiers, and the potential risks to confidentiality that may arise from the linked datasets.

Researchers should consider whether the data linkage is likely to produce identifiable information. In such cases, the researcher must satisfy the REB that the data linkage is essential to the research and that appropriate security measures will be implemented to safeguard information.

GUIDANCE NOTE #8: DOCUMENT RETENTION

In accordance with the Fraser Health Research Policy, research data should be retained for a minimum of 5 years after study completion in order to ensure the integrity of the research and any resulting publications. Funding agencies and academic journals may have longer requirements. For clinical trials regulated by Health Canada, the data must be retained for a minimum of 25 years. The Principal Investigator is responsible for maintaining data following study completion.

GUIDANCE NOTE #9: USES OF DATA AFTER THE STUDY IS COMPLETED

In accordance with Article 4.8 of the TCPS 2, researchers have an ethical responsibility to make reasonable efforts to publically disseminate the results of the study in a timely manner in order to ensure equitable distribution of research benefits. It is ethically unacceptable to prohibit or place undue limitations on the publication or dissemination of research findings.

Researchers must also disclose how research results will be returned to participants. Academic publications and presentations are often inaccessible to participants. Researchers should consider forms of dissemination that are meaningful and culturally relevant to the participants.

Any anticipated future or secondary uses for the data following study completion should be disclosed in the initial application, including how participant consent will be sought. If consent for future uses of data will be sought at the outset, the consent form must describe such uses.

9.1 Open Access:

Journals and funding agencies are increasingly requiring researchers make their data publically available in a research repository. There are numerous benefits to such open access repositories, including minimizing duplication of research and maximizing the benefits that result from data collection. However, open access can create additional privacy and confidentiality concerns, and not all forms of data are appropriate for inclusion in research repositories. Many journals and funding agencies do make

exceptions to open access policies when such access would compromise participant confidentiality and/or participant trust in the researcher.

The consent form must disclose all future uses of the data, including possible open access data repositories. This disclosure should specify what information will be included and how it will be de-identified, and risks of re-identification that may result, and a clear statement that data cannot be withdrawn once it is made publicly available.