Brandon University Research Ethics Committee (BUREC)
Standard Operating Procedure

Data Security, Transporting Data, and Data Retention

General Information:

The collection, use and disclosure of Identifiable Information are regulated by the *Tri Council Policy Statement: Ethical Conduct for Research Involving Human (TCPS2-2018)* and by the Freedom of Information and Protection of Privacy Act (FIPPA). Researchers must comply with these regulations.

As per Chapter 5 – Privacy and Confidentiality – of the *TCPS2-2018*:

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
Security refers to measures used to protect information. It includes physical, administrative and technical safeguards. An individual or organization fulfills its confidentiality duties, in part, by adopting and enforcing appropriate security measures. Physical safeguards include the use of locked filing cabinets, and the location of computers containing research data away from public areas. Administrative safeguards include the development and enforcement of organizational rules about who has access to personal information about participants. Technical safeguards include use of computer passwords, firewalls, anti-virus software, encryption and other measures that protect data from unauthorized access, loss or modification.

Identifiable Information
Where researchers seek to collect, use, share and access different types of information or data about participants, they are expected to determine whether the information or data proposed in research may reasonably be expected to identify an individual. For the purposes of this Policy, researchers and REBs shall consider whether information is identifiable or non-identifiable. Information is identifiable if it may reasonably be expected to identify an individual, when used alone or combined with other available information. Information is non-identifiable if it does not identify an individual, for all practical purposes, when used alone or combined with other available information. The term “personal information” generally denotes identifiable information about an individual. The assessment of whether information is identifiable is made in the context of a specific research project.

Types of Information
Researchers may seek to collect, use, share and access different types of information about participants. Such information may include personal characteristics or other information about which an individual has a reasonable expectation of privacy (e.g., age, ethnicity, educational background, employment history, health history, life experience, religion, social status).

For the purposes of this Policy, researchers and REBs shall consider whether information proposed for use in research is identifiable. The following categories provide guidance for assessing the extent to which information could be used to identify an individual:

- **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 re-identification 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.

Transportation of Data:

All information collected for research purposes, whether identifiable, coded, anonymized or anonymous, should be handled with care in order to protect both the researcher and the participant, and promote research integrity.

Always ensure materials (i.e., paper, devices and/or media) and files (i.e., electronic) are securely transported and/or transmitted. Standard general guidelines include:

- Taking the most direct route to the destination and avoiding stops in transit;
- Transporting materials in a secure/closed container or locked vehicle (i.e., if transporting in a car, lock them in the trunk) or on one's person (i.e., in a purse/bag/carry-on luggage);
- Being discreet when in transit or in public to avoid drawing attention to the materials (e.g., concealing a device in an unmarked bag or container, avoiding use in public);
- Never leaving materials unattended in public areas or transport vehicles (i.e., remove from vehicle as soon as possible);
- Restricting access to materials when off site (e.g., locking devices in a cabinet, password-protecting documents, or taking other steps to limit access by unauthorized individuals);
- Using institutionally-sanctioned systems for sharing electronic information, wherever possible.
- Avoiding use of email to transmit study records whenever possible as email is not a secure method of communicating.

Additional recommendations for the transport/transmission of study records containing Identifiable Information includes:

- Only remove paper or electronic devices/media containing identifiable information from Brandon University premises and/or make copies of identifiable information saved to the Brandon University server in the following limited circumstances:
  - The information is necessary to complete approved research procedures in a timely manner, including, but not limited to:
    - Transporting/transferring materials between university sites;
    - Taking identifiable information into the community or collecting identifiable information in the community during the course of the approved research.
  - Only the minimum amount of information needed to complete the task is copied or collected;
- Study records remain in the possession of the authorized individual (e.g., researcher) at all times, unless a contracted or reputable service is used for transportation (e.g., storage or destruction vendor, Canada Post, courier, secure fax, web form, secure file transfer, encrypted email, etc.);
- Information is de-identified prior to copying or at the time of collection OR, if de-identification is not possible, electronic devices (e.g., laptop) or media (e.g., USB key) on which information is stored are encrypted and password protected;
- Information is only removed for the minimum amount of time necessary to complete the task and;
- Information stored on paper is returned to Brandon University to be secured in a locked filing cabinet, and information stored on portable electronic devices is removed from electronic devices or transferred to a secure network and/or password-protected and encrypted folder as soon as it is no longer needed.

Storage, Retention, and Destruction of Records

Storage of Research Records

For Paper Files:

- If collecting identifiable information:
  - Keep identifying information separate (on a master list) from study data. Replace identifiers (e.g., name, full date of birth) with a unique study ID number or pseudonym. These identifiers should be kept separate from the study data and linked to study data by study number or pseudonym only (see "coded information" described above).
  - Lock identifiable records (e.g., signed consent forms, master list) securely in a filing cabinet separate from study data.
- If collecting identifiable, de-identified (i.e., coded or anonymized), or anonymous information:
  - Store study data on Brandon University premises, or if disclosed in the REB application and Letter of Information and Consent, transfer to a third-party (e.g., sponsor, funder, other research site, regulator, etc.) using the transport/transmission guidelines above;
  - Store study records in a locked cabinet, container, and/or room, whose access is restricted to study team members;
  - Access to study records must be limited to authorized personnel who are listed in the REB application form and Letter of Information and Consent.

For Electronic Files:

- If collecting identifiable information:
  - Keep identifying information separate (i.e., on different drives, in different folders) from study data. Replace identifiers (e.g., name, full date of birth) with a unique study ID number or pseudonym. These identifiers should be kept separate from the study data and linked to study data by study number or pseudonym only.
- If collecting identifiable, de-identified (i.e., coded or anonymized), or anonymous information:
  - Store electronic files on a secure Brandon University sanctioned server or on an encrypted and password protected device (removable media or portable device, e.g., flash drives, USB-connected hard drives, CDs, DVDs, BLueRay, SD cards, etc. OR mobile devices, e.g., laptops, tablets, mobile phones, etc.);
  - If study records will be stored on a server NOT hosted by Brandon University (e.g., SurveyMonkey, etc.) two methods of securing data are required (e.g., encryption and password protection);
  - Access to study records must be limited to authorized personnel who are listed in the REB application form and Letter of Information and Consent;
  - When transferring electronic files to a third-party (e.g., sponsor, funder, other research sites, regulator, professional transcription company, etc.) as disclosed in the REB application and Letter of Information and Consent, protect the files with encryption and password-protection and restrict access to the password only to those third parties.

Retention of Research Records

For data integrity, auditing purposes, and compliance with regulatory guidelines (e.g. granting agencies), researchers should apply Tri-Agency policies on data retention. For more information, visit: http://www.science.gc.ca/eic/site/063.nsf/eng/h_547652FB.html

The TCPS 2 does not specify the required length of time for retention of research data. Data retention periods tend to vary depending on the research discipline, research purpose and kind of data involved. TCPS 2 underscores the importance of data retention as a matter to be considered by research ethics boards in their review of studies that collect identifiable personal information about research participants (see application to Article 5.3) In TCPS 2, a number of factors are relevant to defining periods of data retention. Researchers' plans for preserving or destroying participants' data should be appropriate to the field of research in light of its best practices and professional, ethical and legal norms. For example, under Division 5 of the Health Canada Food and Drug Regulations which pertains to clinical trials of drugs, sponsors are required to maintain records for a period of 25 years. As another example, in the Tri-Agency Statement of Principles on Digital Data Management CIHR requires grant recipients to retain original data sets arising from CIHR-funded research for a minimum of five years after the end of the grant.

Destruction of Research Records

Note: Recycling is not an appropriate method of destruction of identifiable information.

Portable storage devices and Paper Records:

- Shredders: There are many types of shredders on the market that can be used to dispose of CDs, magnetic tape, etc.

Removing data from hard drives

- Workstations: Contact the BU Helpdesk for options to fully "sanitize" the hard drive.
- Servers: Contact the BU Helpdesk for options for the operating system in use.

Adapted from the Western University Guidance Document "Confidentiality and Data Security"

Approved – August 31, 2020