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) 2014 and by the Freedom of Information and Protection of Privacy Act (FIPPA) 2015. Researchers must comply with these regulations.

Identifiable Information: Information that may reasonably be expected to identify an individual, alone or in combination with other available information, is considered identifiable information. There are two types of identifiable information:

Directly Identifying information (Personal Identifiers) – the information identifies a specific individual through direct identifiers (e.g., full name, employee ID, student ID, medical number, S.I.N., driver's license, specific types of research data (participants of research study, employees, students, passwords).

Indirectly identifying information (Personally Identifiable Data) – the information can reasonably be expected to identify an individual through a combination of indirect identifiers (birth date, gender, etc.)

Personal Identifying information should be collected at the lowest level of identifiability possible (e.g., initials instead of name, age instead of full date of birth, etc.) and only be kept as long as necessary.

At Western University, the collection, use, storage, disclosure, retention and destruction of personal identifying information is governed by institutional policy (e.g., MAPP 1.23, 1.30) and the guidelines provided by Information Security (data classification, Data Handling Standards), Western Libraries for Information on Research Data Management Guidelines and Archiving.

Protection of Identifiable Information is an expectation of all individuals conducting research at, or under the auspices of Western University.

A. Transporting of Study Data

The recommendation for the transport of study data containing Identifiable Information is:

Only remove paper or electronic devices/media containing identifiable information from Western University premises and/or make copies of identifiable information saved to the Western 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 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 data remain in the possession of the individual 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 Western University and removed from electronic devices and media as soon as it is no longer needed.

Secure materials (paper, devices and/or media) when removing from Western University premises/servers by using appropriate safeguards, including:

- 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);
- 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 or taking other steps to limit access by unauthorized individuals).

B. Storage, Retention and Destruction of Study Data

Storage of Study Data:

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. These identifiers should be kept separate from the study data and linked to study data by study number only.

- If collecting identifiable or de-identified information:
  - Store study data on Western premises or, transfer to a third-party (e.g., sponsor, funder, other research site, regulator, etc.) as disclosed in this application;
  - Store study data in a locked cabinet, container, and/or room, whose access is restricted to study team members.
  - Access to study data must be limited to authorized personnel

For Electronic Files

- If collecting identifiable information,
  - Keep identifying information separate (on different drives) from study data. Replace identifiers (e.g., name, full date of birth) with a unique study id number. These identifiers
should be kept separate from the study data and linked to study data by study number only.

- If collecting identifiable or de-identified information:
  - Store electronic files on a secure Western University server or on an encrypted and password protected device (removable media or portable devices (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 data will be stored on a server NOT hosted by Western (e.g., SurveyMonkey, DropBox, iCloud, etc.) two methods of securing data are required (e.g., encryption and password protected);
  - Access to study data will be limited to authorized personnel;
  - When transferring electronic files to a third-party (e.g., sponsor, funder, other research sites, regulator, etc.) as disclosed in this application, password-protect the files and restrict access to the password only to those third parties.

Retention of Study Data:
The Office of Research Ethics requires study data (identifiable and de-identified) to be maintained for a minimum of 5 years.

Destruction of Study Data:
Use Western University’s Information Security procedures/guidelines (data classification-destroying) for recommended practices for destroying data and/or data devices

NOTE: RECYCLING IS NOT AN APPROPRIATE METHOD OF DESTRUCTION OF IDENTIFIABLE INFORMATION.