Western Research

Western University
Room 5150 Support Services Building, 1393 Western Road
London, Ontario, Canada, N6G 1G9
Tel: 519-661-2161
ethics@uwo.ca

Guidance Document	HSREB/NMREB: Confidentiality and Data Security
Effective Review	Delegated & Full Board
Version Date	August 21, 2017

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 Identifiable 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 number, contact information, photos, recordings, etc.).
>
> **Indirectly Identifiable Information** (Personally Identifiable Data) – the information can reasonably be expected to identify an individual either alone or through a combination of indirect identifiers (e.g., birth date, postal code, etc.). Indirectly identifying information may vary depending on the context of the research and the population under investigation. For example, in some samples, age, gender and ethnicity (basic demographic information) could potentially identify a participant. In others, professional position/rank could identify a participant, either alone or in combination with other information. Consider all information that will be collected from participants and determine whether there is a reasonable possibility that it may identify a participant.

Identifiable 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.

Coded Information: direct identifiers are removed from the information and replaced with a code (e.g., unique study ID, pseudonym). 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 name so data can be re-linked if necessary; i.e., master list).

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.

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.

Western University
Room 5150 Support Services Building, 1393 Western Road
London, Ontario, Canada, N6G 1G9
Tel: 519-661-2161
ethics@uwo.ca

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

A. Transportation and Transmission of Study Records

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 (contact Western Technology Services [WTS] for more information):
    - Walter (machine name) → Network Attached Drives
    - On Premises (Western) SharePoint → Information available here: http://www.uwo.ca/its/oncampus_onedrive/index.html
    - Off Premises (Cloud) → contact WTS to confirm whether this is an appropriate option given the nature of your data
    - Western's Learning Management System OWL → contact WTS to confirm whether this is an appropriate option given the nature of your data
- 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 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/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;

Western University
Room 5150 Support Services Building, 1393 Western Road
London, Ontario, Canada, N6G 1G9
Tel: 519-661-2161
ethics@uwo.ca

- 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 Western 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.

B. Storage, Retention and Destruction of Study Records

STORAGE OF STUDY 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 Western 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 Western University sanctioned server (e.g., Western drives, OWL, Qualtrics) 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.));

Western University
Room 5150 Support Services Building, 1393 Western Road
London, Ontario, Canada, N6G 1G9
Tel: 519-661-2161
ethics@uwo.ca

- If study records will be stored on a server NOT hosted by Western (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 STUDY RECORDS:

For Directly or Indirectly Identifiable Study Records

- For data integrity, auditing purposes, and compliance with regulatory guidelines (e.g., granting agencies), the Non-Medical(NM)/Health-Science(HS)Research Ethics Board requires that the PI retain identifiable study records for seven (7) years (as per Western University's Faculty Collective Agreement), after which time this information must be destroyed. If the research study is regulated by Health Canada the data must be retained for 25 years. If the research study is being conducted where Lawson Health Research Institute has institutional oversight, their data retention policy is 15 years. The only exception to this is if an extension is requested and justified in the REB application form and participants are notified in the Letter of Information and Consent.

For Anonymized and Anonymous Study Records

- For data integrity, auditing purposes, and compliance with regulatory guidelines (e.g., granting agencies), the Non-Medical(NM)/Health-Science(HS)Research Ethics Board requires that the PI retain de-identified and anonymous study records for a minimum of seven (7) years (as per Western University's Faculty Collective Agreement), but may be retained indefinitely if desired by the researcher. (However, the data can only be used to future research if participants consented to this additional use of their data during the consent process.). If the research study is regulated by Health Canada the data must be retained for 25 years. If the research study is being conducted where Lawson Health Research Institute has institutional oversight, their data retention policy is 15 years.

DESTRUCTION OF STUDY RECORDS:

Refer to Western University's Information Security procedures/guidelines (data classification-destroying: http://security.uwo.ca/information_governance/standards/data_handling_standards/destroying.html) for recommended practices for destroying study records and/or devices. The PI is responsible for complying with all current institutional policies at the time of destruction.

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