University of Manitoba | Human Research Ethics

Human Research Ethics - Fort Garry
66 Chancellors Circle
Winnipeg, MB R3T 2N2
humanethics@umanitoba.ca

Data Storage Guidelines for Research with Human Participants

Introduction

The University of Manitoba has created general guidelines to help researchers share and store university and research data using the appropriate tools. Refer to those guidelines and the data classifications for research that does not include human research data.

For guidelines on storing data from research with human participants, refer to this document. These guidelines were created with the help and support of the Access and Privacy Office, Information Services and Technology Office, UM Libraries Administration Office as well as the Research Ethics Boards (REB).

Your research data may include multiple risk levels. Use the consent form statement for the highest risk of data you will collect. Note, you may need to add additional statements to the consent form sample if other parties or institutions are involved (e.g., sponsor, lead/coordinating site, etc.). Sometimes this access is for monitoring or audit purposes (as required by the protocol and/or agreement) and sometimes we are required by the agreement to send the data to these other institutions.

Consult with the appropriate REB office if your data cannot be stored within these approved platforms.

Data Management Plan

Research Data Management (RDM) is an important component of ethical research practice. Consider completing a data management plan (DMP) along with your ethics submission to ensure you have considered all aspects of data management, including storage, sharing and access for your upcoming research project.
Resources:

- DMP Assistant (A Canadian data management planning tool)
- RDM Support at UM

Types of Information

Refer to the below definitions of the types of information researchers may collect as per the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2 2018):

Anonymous – information never had identifiers associated with it and the risk of identification of individuals is low or very low.

Confidential- safeguard entrusted information from unauthorized access, use, disclosure, modification, loss or theft.

Anonymized- 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.

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

Risk Levels

Low Risk: Data that does not reasonably identify individuals or groups. Data that has been permanently stripped of identifiers. Data that does not contain confidential, private, or otherwise sensitive data. Could be publicly available data.
There is no significant risk from disclosure, loss, or unauthorized release of this data.

Examples:

- anonymous surveys where no identifying information is collected
- anonymized data set where all identifiers have been permanently removed and re-linkage would not be possible.

Medium Risk: Identification information has been separated from the data. Participants have consented to waive their confidentiality. Original (raw) data may be considered confidential, private, sensitive.
There is limited risk from disclosure, loss, or unauthorized release of this data.

Examples:

- Excel sheet with participant ID and research data
- interview transcript with names replaced with pseudonyms
- interview transcript with participant who has waived their confidentiality and would like their real name used in publications.

High Risk: Identifiers remain or (re)identification is possible or probable. Data contains confidential, private, sensitive information. Participants may be vulnerable and/or harmed in case of breach. Data may include self-reported personal health information.
Disclosure, loss, or unauthorized release of this data may result in risk for the participant, the researcher, and potentially the institution including reputational damage, professional or personal disruption, financial consequences, and legal liability.

Examples:

- Audio and/or video files
- participant ID key (i.e., excel sheet) that includes participants ID (e.g., name, email, address and/or phone number).

Extreme Risk: Data acquired through agreement of custodian barring further use or retention. Identifiers remain or (re)identification possible/probable. Data contains confidential, private, sensitive information. Participants are vulnerable and would be harmed in case of breach.
Disclosure, loss, or unauthorized release of this data may result in significant risk for the participant, the researcher, and potentially the institution including reputational damage, significant professional or personal disruption, financial consequences, and legal liability.

Examples:

- Data held at MCHP
- data that is collected through chart review at a medical institution.

Data Storage, Back Up, Sharing, Retention, and Destruction

Risk Level	Process
Low	Storage – Physical Documents In a secure location with access restricted to research team members only (i.e., personal office)
	Storage & Backup – Virtual Documents On encrypted/password protected devises such as USBs or laptops. However, using a network drive or UM Cloud service is preferred. Cloud storage for research data is limited to OneDrive and SharePoint (as authorized/supported by UM). Data cannot not be stored on any other Cloud server.
	Sharing/Transfer Using a UM email account and/or an authorized cloud service. Consider sharing links instead of data files to minimize risk.
	Deposit & Access Can be deposited with no restrictions within reasonable time frame. Secondary data use may require REB approval.
	Retention & Destruction May be retained indefinitely for discovery, access, archival purposes with an appropriate statement on the consent form

Risk Level	Process
Medium	Storage – Physical Documents In a secure location with access restricted to research team members only. Two levels of restriction required (i.e., locked office door and locked filing cabinet).
	Storage & Backup – Virtual Documents Data must be stored in secure locations (i.e., UM network drives or authorized/supported UM Cloud services) or on a Secure Research Environment (SRE) (e.g., RedCap). Encrypted removable storage devices such as external hard drives and USB are permitted but not encouraged due to risk of loss/damage.
	Sharing/Transfer Encrypted and password-protected files can be shared via UM email and authorized/approved cloud services or collaboration sites. Consider sharing links instead of data files to minimize risk.
	Deposit & Access Consent must be obtained for deposit. De-identified data can be deposited with no restrictions within reasonable time frame. Secondary use requires REB approval.

	Retention & Destruction May be retained indefinitely for discovery, access, archival purposes with an appropriate statement in the consent form.

High	Storage – Physical Documents Located in secure location on UM campus with access restricted to limited number of research team members only. Two levels of restriction required (i.e., locked office door and locked filing cabinet).
	Storage & Backup – Virtual Documents Data must be stored in secure locations (i.e., UM network drives or authorized/supported UM Cloud services) or on a Secure Research Environment (SRE) (e.g., RedCap). Encrypted removable storage devices such as external hard drives and USB are permitted but not encouraged due to risk of loss/damage. Data cannot be stored on personal devices.
	Sharing/Transfer Encrypted files can be shared with team members through authorized/approved UM cloud services. Consider sharing links instead of data files to minimize risk. Connect with the REB to discuss other methods if necessary.
	Deposit & Access Consent must be obtained for deposit. De-identified data can be deposited with restricted access as evaluated by data custodian. Data may be separated into sets depending on use cases as documented in REB protocol. Secondary use requires REB approval.
	Retention & Destruction May be retained indefinitely for discovery, access, archival purposes with appropriate justification to REB and with appropriate statement in the consent form.

Extreme	Storage – Physical Documents Located in secure location on UM campus with access restricted to limited number of research team members only. Two levels of restriction required (i.e., locked office door and locked filing cabinet).
	Storage & Backup – Virtual Documents Data must be stored in secure locations and must be encrypted (i.e., UM network drives or authorized/supported UM Cloud services) or on a Secure Research Environment (SRE) (e.g., RedCap). Data cannot be stored on personal devices.
	Storage – when data is acquired through an agreement Where your research utilizes data from other parties, you may need to manage the information/data in accordance with that party's policies, procedures, or in line with any contractual obligations that the party obligates you to utilize. Refer to your agreement for more information.
	Sharing/Transfer

	Encrypted files can be shared with team members through authorized/approved UM cloud services. Consider sharing links instead of data files to minimize risk. Connect with the REB to discuss other methods if necessary. Agreements must be revised to ensure data sharing or secondary use are approved, as applicable.
	Deposit & Access Data should not be deposited beyond direct storage and access needs of the research team.
	Retention & Destruction Data may need to be destroyed at earliest opportunity, in accordance with contractual requirements.