University of Manitoba | Research Ethics and Compliance

Human Ethics - Fort Garry
208-194 Dafoe Road
Winnipeg, MB R3T 2N2
T: 204 474 8872
humanethics@umanitoba.ca

Guidelines for Virtual Research Involving Participants

The University of Manitoba prefers the use of Microsoft (MS) Teams or University of Manitoba (UM) Zoom to conduct virtual research. If these options do not work for your study, please email the research ethics board office affiliated with your study (Fort Gary Campus - humanethics@umanitoba.ca ; Bannatyne Campus – bannreb@umanitoba.ca) with proper justification on a different platform to discuss next steps.

In addition to MS Teams, the University of Manitoba has acquired a university wide license for Zoom. UM Zoom can be used by students and employees with a UM email address and is one of the preferred platforms of the REB. Researchers must use UM Zoom to collect research data rather than personal Zoom accounts.

Additional care must be taken when using videoconferencing platforms to collect research data. The following steps must be taken to ensure data security and to maintain participant confidentiality.

Security Tips

Information for participants:

Providing the following information to participants prior to data collection will help maintain confidentiality:

1. Suggest participants use a nickname or initials instead of their full name.
2. Advise participants that they can keep their cameras off, if they wish.
3. Suggest participants join the meeting in a private location where they will not be disturbed or overheard.
4. Where multiple participants are present (ex. focus groups), remind participants that the information discussed should be held confidential and not be shared outside of the session.
5. Unauthorized recordings are not allowed. In the case of focus groups, it should be made clear that the researcher cannot guarantee that other participants will not record the session.

During the meeting:

1. Lock the meeting once in progress – locking a meeting ensures that no new participants can join.
2. Manage Participants:
   a. Prevent screen sharing – restrict screen sharing to the host, unless required for your study.
   b. Disable private chat - Disabling private chat prevents participants from privately messaging other participants, but still allows participants and the host to send private messages to each other.
   c. Turn off annotation, unless approved in your ethics application.
   d. Mute participants until ready to protect participant privacy
   e. Remove participants – if necessary, participants can be removed from a meeting. They will be unable to re-join unless this setting is enabled in Zoom.

Instructions on how to manage Zoom settings can be found at https://umanitoba.ca/about-um/tools-working-remotely/um-zoom-security

Instructions on Teams meetings can be found at https://umanitoba.ca/microsoft-365/build-your-skills-microsoft-teams

Zoom Tips before starting:

1. Please ensure you have migrated your account to the UM Zoom account.
2. If you plan to record to the Zoom cloud, ensure you have enrolled in multi-factor-authentication (MFA). https://umanitoba.ca/multi-factor-authentication
3. Do not use Personal Meeting IDs – schedule meetings with a randomly generated meeting ID so only invited attendees can join.
4. Only share meeting links with the selected participants - use secure UM email accounts to share meeting links, not social media or the web.
5. Password protect meetings so that only those with the password can access the meeting room.
6. Do not allow others to join a meeting before the host – this feature is available under 'Account settings'.
7. Use a Waiting Room – a virtual waiting room allows the host to invite guests into the main meeting when ready.
8. Authentication must be on. This means only authenticated users can access meetings (users with @umanitoba.ca or @myumanitoba.ca email accounts). Participants can be added as exceptions through the UM Zoom Web portal. For guidance on how to add an authentication exception for research participants please view the following link: https://umanitoba.ca/sites/default/files/2021-09/zoom-authentication-exception.pdf
9. Disable video if it is not required for research purposes.

Data Storage and Sharing for Recordings

Teams recordings are available in different places depending on the type of meeting. The recording is processed and saved to SharePoint if it was a channel meeting (channels are subgroups within teams) or OneDrive if it was any other type of meeting. The meeting recording shows up in the meeting chat or channel conversation (if you're meeting in a channel). Guests and external attendees can view the recording only if it's explicitly shared with them. Please turn this off unless it was approved in your ethics application. Teams will record audio and video together into one file.

UM Zoom offers two storage options: (i) local drive on a UM managed computer; (ii) cloud storage. There are benefits to either choice depending on the nature of your research as well as some considerations.

Locally Stored Recordings on UM-managed computer:

- Computer must have disk encryption enabled
- Both audio and video are captured simultaneously (and cannot independently selected until after the recording has stopped)

- Recordings should be transferred at the earliest opportunity to the UM-approved, primary storage location, and no later than one week after recording. For storage service recommendations, see below.

Recordings stored in Cloud:

- UM Zoom must be used with multi-factor authentication (MFA) enabled
- Recordings should be transferred at the earliest opportunity to the UM-approved, primary storage location, and no later than one week after recording. For storage service recommendations, see below.
- Researcher can choose, at the time of recording, what form of recording will take place (ex., can choose to capture only audio)
- Provides additional security by reducing data breach or data loss risk via account compromise or device failure/theft

In your ethics application, please indicate which recording option has been selected and why.

Consider the following services for long term storage of video/audio recordings:

- **Network drives (i.e., H drive, S drive).**
    - UM managed device- your device has Microsoft Bitlocker enabled. No further steps are required.
    - Personal device- the recordings and chat files must be encrypted using 7zip. More information on how to encrypt individual files can be found at the end of this document.
- **UM supported cloud service**s with MFA enabled (OneDrive, SharePoint, Microsoft Teams). No further steps are required.
- **Sharing/transferring electronic files**. When files are in transit (ex. sent from one investigator to another), they must be encrypted. Please use 7zip to encrypt these files before transfer. If possible, use UM supported cloud services (ex. SharePoint) instead of sending documents through email etc. Your data transfer method should be clearly outlined in your ethics application.

Recording Settings

Required settings in Zoom:

- Ensure that ‘Cloud recording’ is OFF, unless using cloud recordings.
- Ensure ‘Automatic Recording’ is OFF
- To ensure that cached cloud recording files are deleted, ‘**Auto delete cloud recordings after days’** should be set to ON with the deletion occurring no more than 7 days after recording.
- Ensure ‘IP Address Access Control’ is OFF
- Ensure ‘Recording disclaimer’ is set to ON
- Ensure ‘Ask participants for consent when a recording starts’ is set to ON
- Ensure ‘Ask host to confirm before starting a recording’ is set to ON
- Ensure ‘Hosts can give participants the permission to record locally’ is OFF

Transparency

The consent form should indicate if audio and/or audiovisual recording will take place as well as how and where the recording and any transcriptions will be stored. Participants should explicitly consent to audio and/or audiovisual in the consent form using a checkbox.

Consent forms should clearly state that UM MS Teams or UM Zoom will be used, and that the researcher cannot guarantee complete privacy of the data collected through these mediums. In the case of focus groups, the consent form should also clearly state that the researcher cannot guarantee that other participants will refrain from recording the session in means external to MS Teams or Zoom.

Withdrawing

In your ethics application and consent forms, please clearly state what will happen to the recordings in the event the participant decides to withdraw during the meeting or after. In the case of locally stored recordings, if only audio will be used for analysis, please indicate what will happen to the video recording.

For group meetings or focus groups, please be clear with participants on the limitations of the recordings in the consent form and when they withdraw. While you may be able to remove their quotes from the transcript, it is likely not feasible for you to remove them from the video and/or audio recording. If you are sharing the recordings publicly or archiving this information, please only include parts of the recording from consenting participants or edit the full recording to remove information from the individual who has withdrawn.

How to Encrypt and Decrypt Files

Caution: An encrypted copy of a file is not readable without the password. Ensure the recipient can decrypt the file before deleting the unencrypted original.

Note: the following methods were tested and verified to work on Windows 10 Enterprise and MacOS Mojave.

Windows

7zip is a free zip archive utility for Windows that can encrypt files using AES-256-bit encryption. If you do not have a copy installed and to not have the rights to install it, please contact servicedesk@umanitoba.ca to install it for you.

ENCRYPT

1. Download 7Zip and install
2. Right mouse click/7-Zip/Add to Archive on the file you wish to encrypt.

3. In the bottom right corner of the 7zip menu under ‘Encryption’ enter a password that meets the U of M password standard then click ‘ok’ to encrypt the file.
4. 7zip will create an encrypted copy of the file with a .7z as the file extension

DECRYPT

1. Ensure 7Zip is installed on the device you are using to open the file.
2. Right mouse click/7-Zip/Open Archive and enter the password that was set during encryption.

MacOS

ENCRYPT

1. Click on Terminal from Applications>Utilities
2. Type: zip -e filename.txt filetoencrypt.txt (where filename.zip is the name of the encrypted file you want to create and filetoencrypt.txt is the name of the file you want to encrypt).
3. Enter a password that meets the U of M password standard

DECRYPT

1. Click on Terminal from Applications>Utilities
2. Type: unzip filename.zip (where filename.zip is the name of the encrypted file)
3. Enter the password used to encrypt the file.