University of Manitoba | Human Research Ethics

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

Guidelines for Virtual Research Involving Participants

The University of Manitoba recommends using Microsoft (MS) Teams or University of Manitoba (UM) Zoom for conducting virtual research activities. If these platforms are not suitable for your study, please contact humanethics@umanitoba.ca with a justification for using an alternative platform so that next steps can be discussed.

In addition to MS Teams, the University of Manitoba provides a university-wide Zoom license. UM Zoom is available to all students and employees with a UM email address and is one of the Research Ethics Board's preferred platforms. Researchers must use UM Zoom—not personal Zoom accounts—when collecting research data.

When using videoconferencing platforms for research purposes, additional precautions are required to protect data security and maintain participant confidentiality. Researchers must follow the steps outlined below to ensure these standards are upheld.

Security Tips

Information for participants:

Providing the following information to participants before data collection will help protect their confidentiality:

1. Encourage participants to use a nickname or initials rather than their full name.
2. Inform participants that they may keep their cameras turned off if they prefer.
3. Recommend that participants join the meeting from a private location where they will not be interrupted or overheard.
4. For sessions involving multiple participants (e.g., focus groups), remind them that all information shared is confidential and should not be disclosed outside the session.
5. Advise that unauthorized recordings are prohibited. In focus groups, clarify that the researcher cannot guarantee that other participants will refrain from recording the session.

During the Meeting:

1. **Lock the meeting once it has begun** – Locking the meeting ensures that no additional participants can join after the session is in progress.
2. **Manage participants effectively:**

a. **Restrict screen sharing** – Limit screen sharing to the host unless participant sharing is required for your study.
b. **Disable private chat** – Turning off private chat prevents participants from messaging each other privately, while still allowing private messages between the host and individual participants.
c. **Turn off annotation tools** unless their use has been approved in your ethics application.
d. **Mute participants on entry** to help protect privacy and reduce disruptions.
e. **Remove participants if necessary** – Participants can be removed from the meeting when required. Note that they cannot rejoin 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/information-services-technology/welcome-microsoft-365/build-skills-microsoft-teams

Zoom Tips Before Starting:

1. Confirm your account is migrated to the UM Zoom system to ensure full access to university-supported features.
2. Enroll in multi-factor authentication (MFA) if you plan to record sessions to the Zoom cloud.
3. Avoid using Personal Meeting IDs (PMIs). Schedule meetings with randomly generated IDs so only invited participants can join.
4. Share meeting links only with selected participants and use secure UM email accounts—not social media or public websites—to distribute them.
5. Password-protect all meetings to ensure only individuals with the password can enter.
6. Disable the “join before host” option in your account settings to prevent participants from entering the meeting room early.
7. Use the Waiting Room feature so you can admit participants into the meeting when you are ready.
8. Enable authentication. This setting restricts access to authenticated users (those with @umanitoba.ca or @myumanitoba.ca email accounts). You may add authentication exceptions for research participants through the UM Zoom web portal. Guidance is available here: https://umanitoba.ca/sites/default/files/2021-09/zoom-authentication-exception.pdf
9. Disable participant video when it is not necessary for your research activities.

Data Storage and Sharing for Recordings

Teams recordings are stored in different locations depending on the type of meeting. If the meeting was held within a channel (a subgroup within a Team), the recording will be processed and saved to **SharePoint**. For all other meeting types, the recording will be saved to **OneDrive**. Recordings will also appear in the meeting chat or, for channel meetings, in the channel conversation. Guests and external attendees can only view the recording if it is **explicitly shared** with them. This option should remain disabled unless your ethics application specifically permits external sharing. Teams automatically records audio and video together in a single file.

UM Zoom provides two options for storing recordings:

1. **Local storage** on a UM-managed computer, or

2. **Cloud storage** within the UM Zoom environment.

Both options have advantages depending on the nature of your research, but each also requires careful consideration regarding security and data management.

Locally Stored Recordings on UM-managed computer:

- The computer used for storing recordings must have disk encryption enabled to ensure the security of research data.
- Audio and video are captured simultaneously, and these components cannot be selected or separated until after the recording has been completed.
- Recordings must be transferred to the UM-approved primary storage location as soon as possible, and no later than one week after the recording. (See the storage service recommendations below.)

Recordings stored in Cloud:

- UM Zoom must be used with multi-factor authentication (MFA) enabled to ensure secure access to the platform and its recording features.
- Recordings must be transferred to the UM-approved primary storage location as soon as possible, and no later than one week after creation. (See storage recommendations below.)
- Researchers may choose the recording format at the time of recording—for example, opting to capture audio only.
- Using UM Zoom with MFA provides enhanced security, helping reduce the risk of data breaches or data loss resulting from account compromise or device failure or theft.

Please specify in your ethics application which recording option you have chosen and provide a rationale for that choice.

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

- **UM supported cloud service**s with MFA enabled (OneDrive, SharePoint, Microsoft Teams). No further steps are required.
- **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.
- **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 must clearly state whether audio and/or audiovisual recording will occur, and describe how and where the recordings and any resulting transcriptions will be stored. Participants should provide explicit consent to audio and/or audiovisual recording by selecting the appropriate checkbox in the consent form.

The consent form should also specify the researcher cannot guarantee complete privacy of data collected through these platforms. For focus groups, the consent form must additionally state that the researcher cannot guarantee that other participants will refrain from making their own recordings outside of 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.