

Conducting Virtual Interviews and Focus Groups

1. **Informed Consent:** Participants should have already consented to participating in the focus group before attending the intervention. A new letter of Information should be emailed/mailed to participants outlining the use of virtual methods, risks related to it; privacy and confidentiality measures. Participants can provide verbal consent to being recorded etc.
If there are participants who need to consent. They can provide verbal consent to participating in virtual focus group after reading the letter of information.

2. **Virtual platforms available for research involving human participants at McMaster:**
Zoom, MS Teams and WEBEX are available through the university and can be used as preferred. Interface specific information and how to securely set up meetings can be found on the following links.
Using Zoom for Research: <https://research.mcmaster.ca/videoconferencing/zoom/>
Using MS Teams for Research: <https://research.mcmaster.ca/videoconferencing/msteams/>
Using Webex for Research: <https://research.mcmaster.ca/videoconferencing/webex/>

3. **Practices for administering online interviews and focus groups**
 - a. *Making the Recording:* The most secure way to audio record interviews/focus groups is to record to your computer or device using an application that directly records the audio to your hard drive. Another option is to record through the online meeting platform (e.g. Zoom) directly to your computer, but most of these platforms only allow for recording video and audio together, not audio separately. Additionally, you will need to confirm that the platform you are using can record directly to your computer as opposed to the platform's server or to a cloud service. Where recordings must be saved to a cloud, they should be downloaded to local storage and deleted from the cloud immediately. As soon as the interview/focus group is finished, the file should be saved to a password protected storage device, e.g. computer, external hard drive, and encrypted. Details about recording and data security information should be included in the Letter of Information. A clear consent statement needs to be included on the Oral Consent Script if audio (and video) recording.
 - b. *Video Recording:* Online platforms make it easy to video record a meeting. Video recording should not be used unless it is essential for your research methodology and clearly justified. Sometimes it is only possible to record video and audio together through the platform and you would need to use a separate application to record audio only. If you do need a video recording, due to methodology or limitations on using a separate application to record audio, then the fact the session will be video recorded needs to be

stated in the Letter of Information and a clear consent statement needs to be included on the Oral Consent Script or Consent Form. Most interviews/focus groups will not need video recording and in those cases the Letter of Information should inform participants that the interview/focus group will be audio recorded only and not video recorded.

- c. *Attendance*: Consider whether participants can choose to join the interview/focus group by audio only, given not all participants may have access to video and there may be limitations to the location from which a participant can join during this time of social distancing. Additionally, in a focus group setting, joining by audio only increases the confidentiality of participation (in conjunction with using a pseudonym) for more sensitive data collection. If joining a session by audio only is not an option, this should be clear in the Recruitment and the Consent materials.
- d. *Participant Recording of Focus Groups*: Any participant could covertly record an in-person focus group if they were so inclined. However, it is even easier to make a good recording of an online focus group without other participants or the researcher knowing, and it could include video. In the section of the Focus Group Guide where you discuss confidentiality with participants, include a statement requesting participants not record the session. Additionally, this risk to participant privacy should be clearly stated in the Letter of Information along with a reminder that researchers cannot guarantee that all participants will refrain from recording the session. For more sensitive data, one-on-one interviews may be preferable to a focus group.
- e. *Privacy Risks from Using Online Meeting/Voice Calling Platforms*: No online platform is 100% secure and so participants should be given enough information to make their own decisions about participation on the selected platform. The Letter of Information should include language that makes it clear what platform(s) is being used, and that no guarantee of privacy of data can be made, so the risks of participation are clear. Here is some sample wording, "This study will use the X platform to collect data, which is an externally hosted cloud-based service. A link to their privacy policy is available here (LINK). Please note that whilst this service is approved for collecting data in this study by the McMaster Research Ethics Board, there is a small risk with any platform such as this of data that is collected on external servers falling outside the control of the research team. If you are concerned about this, we would be happy to make alternative arrangements for you to participate, perhaps via telephone. Please talk to the researcher if you have any concerns."
- f. *Keeping Focus Group and Interview Sessions Private*: Before using online platforms for interviews or focus groups, researchers should become familiar with the settings and invitation options and take steps to prevent unauthorized persons from accessing the

session (e.g. “Zoom bombing”). Most of the time, unauthorized access is due to the meeting link being made public, which should be less of an issue for research as the link should only be shared privately with participants. But participants could accidentally disclose the link, and therefore researchers should be aware of other options to prevent access (e.g. two factor authentication) and to address the situation if someone gains access to a focus group (e.g. have screen sharing turned off, know how to remove someone, etc.). For those using Zoom, there is a guide to preventing unauthorized access posted by the company.