Wayne State University
Institutional Review Board (IRB)

WSU IRB Administration Office
87 East Canfield, Second Floor
Detroit, MI, 48201
313-577-1628
irb.wayne.edu

Virtual Data Collection and Meeting Platforms:

This guidance document lays out a variety of easy steps researchers can take to protect the privacy and confidentiality of research participants. This guidance is applicable to researchers who plan to conduct virtual interviews and focus group sessions using an on-line meeting platform such as Zoom or Microsoft Teams. The general guidelines and best practices described in this guidance document can be applied to other virtual meeting platforms as allowed by the chosen virtual meeting platform's permission. Whatever virtual meeting platform you choose this must be included in the IRB submission with a detailed description of the steps that will be taken to protect the research participants privacy and confidentiality.

As with most online platforms, privacy and security risks exist and when used for research purposes steps can be put in place to minimize these risks.

Privacy & Security Settings to use Before the Meeting Begins:

1. **Create private meetings (Zoom).** When creating a meeting, it is recommended that a new unique meeting code is created for each meeting session. This will ensure that only invited attendees are able to join your meeting. Using your Personal Meeting ID (PMI) that is specifically tied to your account allows anyone with the number to enter your personal meeting at any time. Avoid sharing this number and instead provide a new, private meeting code for each meeting.

2. **Use a meeting password (Zoom).** By using a password, you can ensure that only those with the password are able to enter your meeting. Although the password function can be turned off, all researchers are expected to use this feature. Zoom Meeting Password Instructions.

3. **Use of the Video Camera:** It is recommended that researchers inform participants in advance that cameras will be turned on during the session. Include this information for the IRB submission, Research Information Sheet, and participant communications preparing for the session. Participants should be given the option to decline a researcher's request to turn the camera on during the virtual meeting.

Procedures to protect the confidentiality and privacy of participants.

4. **Waiting Rooms/Lobby:** The virtual waiting room, for example (Zoom) or lobby (Teams) feature can be used as a means to allow participants time to change their names to a pseudonym on their profile before entering the meeting room. This can help protect a research participants' anonymity. Zoom Waiting Room Instructions.

   a. Note: In Microsoft Teams, only individuals who join the meeting as a 'guest' are able to change their name when they join the meeting. If participants join using their own Teams account they may be unable to change their displayed name.

5. **Use of the message feature to conduct anonymous meetings:** If the protocol requires meetings to be conducted anonymously, or the participant requests to remain anonymous, researchers can conduct anonymous meetings with participants by sending a message to participants in the waiting room to remind them to turn off their cameras and revise their profile name using an alias.

6. **Lock meetings (Zoom).** Once all participants have entered the meeting, the host can lock the meeting which will not allow anyone else to join. Instructions provided in Zoom's In-Meeting Security Options.

7. **Hide Profile Pictures (Zoom):** In-meeting security options allow the host to hide all profile pictures which helps to protect a research participants anonymity. Instructions provided in Zoom's In-Meeting Security Options.

8. **Encrypt Research Meetings:** Encryption converts sensitive information or data into a secret code to prevent unauthorized access (Norton, 2023). This is a standard requirement to protect research participants confidentiality. When meetings with research participants occur virtually using the Zoom meeting platform, researchers should encrypt meetings following the instructions provided in Zoom's In-Meeting Security Options.

    a. **Understand what Zoom's encryption policy means.** Although others will not be able to access any audio or video content created from your encrypted meeting, this information is not private from Zoom itself. Please make sure your participants understand this.

9. **Change the background to create privacy:**

    Camera is enabled:

    To protect study participants' privacy, ask that participants to blur their background or use a non-descriptive virtual. Request that participants set-up in a private location where there are not others nearby. If the data collection includes collecting information about the participants environment this collection/observation must be described as part of the study procedures documented for the consent/assent forms.

    Researchers should be in a private location where non research personnel cannot hear or see the session. Researchers should also blur their background or use a WSU background setting.

10. **Recording virtual meetings:** Recording sessions present additional security and privacy risks when not handled properly. To protect research participant's privacy, only use this function only when necessary and in accordance with IRB approval. Audio and video recording a virtual meeting is considered collection of identifiable data. Note: If you only need the audio recording, ask the participant to keep their camera off before you start recording.

a. **Make sure all participants consent to the recording:** Plans to record meeting must be included in the informed consent form or information sheet. Meeting room settings must be set up to require permission and/or alert participants that they are being recorded. Meetings with research participants cannot be recorded if participants inform the researcher that they do not want to be recorded.

   i. Obtaining consent during a virtual meeting for minimal risk research with a waiver of documentation of consent can be done by either sharing your screen to display the IRB approved information sheet and reviewing the information with the participant, or by reading an IRB approved oral consent script to the participant. With both methods, participants will indicate their consent by agreeing to proceed with the interview. Signatures are not documented. You can find an IRB Education On Demand video on the topic of waivers of consent for more information and instructions for requesting a waiver of documentation of consent on the IRB's Education website

b. **Storing Recordings:** Keep in mind that any virtual meeting platform you use will have access to all data stored in their cloud platform when deciding whether to store recorded meetings on the cloud or on your computer. If recordings stored on the virtual meeting platform's cloud will contain individually identifiable data, research participants must be informed that the virtual meeting platform being used will have access to their data for as long as the recording remains stored in the platform's cloud. Recordings stored on Zoom & Microsoft Teams are encrypted. If storing recordings on your computer, they must be saved on an encrypted server. Additional information about storing and protecting data is available in the IRB's Data Collection and Confidentiality Guidance tool located on the IRB Education website.

   i. **Zoom recordings stored on the Zoom cloud** are automatically deleted after 240 days. If the recording is still needed after that time, Zoom will send an email notifying you that you have a recording that will be deleted soon. The email also gives you an option to go in and recover your cloud recordings.

   ii. **Microsoft Teams recordings are stored on SharePoint or OneDrive.** Users can manage the expiration date of meeting recordings. See Microsoft Instructions to Record a meeting in Microsoft Teams

c. **Transcribing the recording:** Whenever meetings are recorded, researchers should promptly transcribe the recording, omitting or obfuscating any unnecessary information and any information given that could identify the participant, or any other individual discussed in the interview or focus group and then promptly destroy the recording as soon as the recording is no longer needed.

IRB Submission

Include the virtual data collection procedures (including the name of the virtual meeting platform that will be used) for the following components of the IRB Submission:

- eProtocol application
    - Study Location, Study procedures, and Procedures to Maintain Confidentiality sections
    - Internet Use in Research Addendum
    - Consent/Assent Forms

Note: The virtual meeting procedures must be carried out as stated in the IRB approved application. If modifications to the virtual meeting procedures are necessary, an amendment must be submitted to the IRB for IRB approval of the updated procedures. Your virtual meeting procedure should include some flexibility to allow you to accommodate research participants' level of comfort with the virtual meeting technology.

Resources:

See the IRB's Data Collection and Confidentiality Guidance Tool for additional information about the IRB's recommended methods to protect the confidentiality of research data.

IRB Education On-Demand Videos located on the IRB Education Website:

- Waivers of Consent
- Fundamentals of the IRB Parts 1, 2 & 3

Additional Zoom & Microsoft Teams guidance and resources is available on the Wayne State University's Computing & Information Technology (C&IT) Zoom website & Microsoft Teams Websites