THE UNIVERSITY OF TENNESSEE CHATTANOOGA

Institutional Review Board
Dept 4915
615 McCallie Avenue
Chattanooga, TN 37403
Phone: (423) 425-5867
Fax: (423) 425-4052
instrb@utc.edu
http://www.utc.edu/irb

Guidance for using Zoom in Human Research Data Collection

As many research studies shift to using Zoom to eliminate the risks of spreading COVID-19 during research with human participants, researchers need to be aware of privacy and confidentiality considerations related to the use of the Zoom platform. The following tips can help maximize privacy and confidentiality during data collection using this resource.

What is Zoom?

Zoom is an online platform that can be used to conduct video meetings, focus groups, and interviews. Zoom is supported by the University of Tennessee system, and Zoom Basic accounts are available to any faculty, staff, and students in the UT system. Individuals do not need an account to participate in a Zoom meeting.

When conducting research, it is strongly encouraged that UTC faculty, staff, and students create and utilize a Zoom account through the UT portal. Creating an account through UT, as opposed to using a personal, non-UT affiliated account, will allow the user to control and modify many more detailed settings that will improve privacy and security. The following guidance is based on the assumption that the user has a UT supported Zoom account.

By default, UT users will have a Zoom Basic account. A Zoom Basic account allows users to host unlimited meetings of 40 minutes in duration with up to 300 participants. UT faculty and staff may request a Zoom Pro account, which will allow users to host unlimited meetings with unlimited duration with up to 300 participants. To request a Zoom Pro account, set up a basic account and then contact the UTC Information Technology with your request to upgrade your account to the Zoom Pro level.

To create an account or log in to Zoom, visit https://tennessee.zoom.us/ and click "Create or Edit Account". Log in with your UTC ID and password. For additional guidance, see UTC Zoom Leader Guide for instructors or Leaders and Zoom Participant Guide (developed by the UTC Walker Center for Teaching and Learning).

Privacy and Security Tips:

1. "Zoom bombing" is when an uninvited and unwanted participant gains access to a private meeting. There are settings in Zoom that can prevent the likelihood of this happening. These include:

i. **Use a Private Meeting Code:** Always create a new private meeting code for each meeting, instead of using your Personal Meeting ID.

ii. **Require a passcode for all meetings.**

iii. **Individual recruiting:** Do not broadly disseminate call details or post them to a public forum, such as a social media account. When possible, hosts should email the participants the details of the meeting directly. If this is not possible, hosts should provide passcodes to participants separately from other meeting details.

iv. **Turn on Waiting Rooms.** This feature ensures that the host must approve each attendee prior to them having access to the meeting.

v. **Lock meetings:** Hosts should "lock meetings" once all participants have entered the meeting, which will not allow new participants to join.

2. To reduce possible exposure of participant confidential information:

   i. **Disable screen sharing for participants.**

   ii. **Disable Zoom file-transfers.**

   iii. **Adjust Zoom settings so that meetings begin with participant video off and audio muted.**

Recording a Zoom meeting:

Recording a Zoom meeting is not always optimal. Doing so requires specific consent from the participant and creates more risks associated with potential loss of confidentiality. The researcher must consider how the resulting data will be secured, who will have access to it, and how and when it will be disposed of. However, should the researcher decide that recording is necessary for the project, the following guidelines must be adhered to:

1. **All participants must expressly consent to being recorded**. Consent language to include on the consent form can be found on the UTC IRB website. The researcher should verbally let the participant know when recording will begin.

2. **Participants should be informed that they are not to record the interview themselves.**

3. **Modify the following settings:** Before the meeting and from the web interface (https://tennessee.zoom.us/account)**, hosts should select "Create or Edit Account," "Settings", "Recording" and modify the following settings:

   Local recording should be 'on'

   Hosts can give participants the permission to record locally should be 'off'

   Automatic recording should be 'off'

   IP Address Access Control should be 'off'

Only authenticated users can view cloud recordings should be 'on'

Auto delete cloud recordings after days should be set to 'on' with **the time range** set to no more than 7 days. This is just to ensure any cached recording files are deleted since you are going to be saving recordings locally.

Recording disclaimer should be set to 'on'.

Ask participants for consent when a recording starts should be set to 'on'.

Ask host to confirm before starting a recording should be set to 'on'.

***NOTE: These settings cannot be changed on the desktop application. You must log into the web interface.*