PEPPERDINE
UNIVERSITY

Researcher Guidance for the Use of Zoom in Data Collection

**This guidance may be updated with additional information as it becomes available.*

Introduction

The use of virtual platforms to conduct research has become increasingly common. The online platform Zoom is a frequently used host for the collection of primary data through interviews and other types of virtual communication. As with most online platforms, privacy and security risks do exist, and researchers need to prioritize participant protections with secure data collection and management.

This guidance document lays out how researchers can change Zoom settings and how to initiate and conduct their Zoom meetings and any recordings through Zoom in order to provide maximum protection to their research participants and the data collected. It also provides guidance for the IRB application submission.

General Considerations in Study Design

1. **Limit research interactions that collect highly sensitive data**. Zoom Inc. may have access to any audio or video collected via its Zoom platform. The free and regular paid versions of Zoom (including your Pepperdine account) are not HIPAA compliant and should not be used for any study involving the collection or use of protected health information (PHI). If you anticipate collecting protected health information, please contact the IRB office to discuss temporary access to Pepperdine Health Care Zoom (with a University issued HIPAA compliant Zoom account) which will restrict data retention timeframes and data sharing.

2. **Limit the use of the record function**. Recording Zoom sessions presents additional security and privacy risks when not handled properly. Only use Zoom's recording function when absolutely necessary and only when official study activities commence (e.g., when you begin asking questions from your prepared questionnaire and not during the set-up or introduction portions of the Zoom meeting).

3. **Minimize the collection of personally identifiable information**. Both voice and video recording are personally identifiable information. These forms of data are vulnerable as they include information about the participant that allows others to identify them. If unauthorized individuals gain access to this data, there could be a breach in confidentiality and privacy agreements, so best practices is to limit the number of identifiers captured in recordings. Remember that if you record from Zoom, both video and audio will automatically be captured. If video is not required for your study, please delete the video file as soon as the recordings are uploaded to the Zoom cloud to minimize identifiers linked to your participants.

How to Address These Considerations in Your IRB Protocol

1. Review the 3 guidelines described above under section the *General Considerations in Study Design*. Make sure to follow guidelines #1 and #2 and consider #3 before finalizing your study protocol.

2. If you are recording with Zoom, then the *Study Procedures(2b)* and *Data Protection/Subject Confidentiality (6b)* sections of your IRB application must address all of the "Privacy and Security Tips" below (#1 through #7). This involves: **1**) describing all 7 considerations in some way within your IRB protocol in the relevant sections, and **2**) making sure your informed consent form addresses #4 – 7 (encryption, consent to record, data stored on Zoom cloud, and the management and use of recorded data).

3. **Additionally, if you think video recording is necessary (and not just audio recording), provide compelling reasoning (e.g., to identify who is speaking in a focus group, if study objectives involve rating or evaluating non-verbal behaviors or observations of an activity or specific actions) as to why your study requires video capture in the *Study Procedures (2b)* section of your IRB application.

Privacy and Security Tips for Recording Audio and Video on Zoom

1. **Create private meetings**. Make sure that a new zoom meeting link and a new password is generated for each participant.

2. **Enable the waiting room function** (available under meeting options). This allows the host to approve each new attendee before they can access the room.

3. **Uncheck the option to "display participants' names in the recording**. The host can change setting in Zoom before starting the meeting so that display names of attendees will not be captured in recordings. This will further protect additional personally identifying data from being collected (such as their full names) in association with their voice and video.

   - Log into Zoom via Web Browser
     - zoom.pepperdine.edu
     - Click Sign in
   - Go to Settings (Left panel)
   - Select Recording (Top tab)
   - Under Advanced cloud recording settings uncheck "Display participants' names in the recording

4. **Explain what Zoom's encryption policy means**. Although other people will not be able to access the audio or video content created from an encrypted meeting (including any recordings using Zoom), this information is not private from Zoom Inc. Please make sure your participants understand this before pressing record in Zoom. Also, you must create a statement communicating this information to participants in the consent form.

5. **Make sure all participants provide verbal consent before you start recording**. In addition to obtaining participants' written consent via the consent form, it is expected that all researchers also verbally consent participants prior to recording by informing them you will be starting the recording and asking them to say "yes" if they agree to being recorded.

6. **Record to Zoom cloud**. All Zoom recorded meetings should be saved to Zoom cloud and not to one's local password-protected computer. If you are using Zoom just to establish a visual connection with the participant and a separate external/USB handheld recorder is used to record audio, this data can be stored on a local password-protected computer, Google Drive (with sharing permissions set properly), and other password-protected storage options if it involves confidential data only and not restricted data. *Please see *Data Handling Guidelines* document for more information.

7. **Only keep video and audio files long enough to enable written transcription of materials**. Once the transcriptions are created, the video and audio files must be deleted from your local drive promptly. If there is any reason to maintain the audio and/or video files, an explanation of why this is necessary to your study must be included in your IRB application along with additional protective measures you will take to reduce the risk of this information being accessed by others. Please see *Security Recommendations for Voice Recordings* document for specific guidance. These details must also be summarized and presented in the consent form so participants are aware of how their recorded data will be managed.

Other Important Notes

1. **Exempt Review Criteria**. The use of Zoom to record audio and video files may be reviewed as an exempt application provided that **1)** all of the considerations above in this document are addressed in a satisfactory manner by the researcher, and **2)** there are no additional foreseeable risks involved in the study. The following are some examples of additional foreseeable risks and are not meant to be comprehensive:

    - The anticipation of more than minimal emotional distress or discomfort from participating (such as answering questions about trauma or mental health conditions)

    - When disclosure of the human subjects' responses outside the research would possibly place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation.

    - The collection of any PHI which is subject to HIPAA regulations. This is restricted data and will require special provisions including the setup of Pepperdine Health Care Zoom for study activities.

2. **Exempt Review IRB Application Sample Language**. Considering your study design, your subject population and the nature of the interview questions (i.e. the degree of sensitivity of the questions asked), if you believe that your study protocol meets criteria **1)** and **2)** from the above *Exempt Review Criteria* section and you want the application to be considered for exempt review, you will need to explicitly include the following text in your IRB application and in your informed consent form under the *Risks and Discomforts (4c)* section (with words in parentheses substituted in the consent form):

    - *"Participating in this research is not likely to cause participants (you) more than minimal emotional distress or discomfort. Also, the researchers do not anticipate that if there is an accidental disclosure of participant's (your) responses (such as a data* *breach despite all protective measures taken), that this would possibly place them (you) at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation*".

You will also need to explicitly include the following text in your IRB application and in your informed consent form under the *Data Protection/Subject Confidentiality (6b)* section (with words in parentheses substituted for insertion in the consent form)

- In IRB protocol: "*Participants will be made aware that Zoom Inc. has access to all audio and video content (including recordings) created through the platform on the written consent form. They will also be verbally made aware of this and asked to verbally consent prior to pressing record during the Zoom meeting*."
- In informed consent form: *"It is important to understand that because we will be recording via Zoom, technically, Zoom, Inc. can have access to your audio and video recordings."*

3. **File Sharing**. If you need to share files among research personnel (all of whom should be disclosed on your IRB application), note that confidential data (most studies excluding those collecting personal health information and when collected data is not considered publicly available information) require password protection for sharing. Therefore, make sure to add to your IRB protocol (and informed consent form) in the *Data Protection/Subject Confidentiality (6c)* question that you will share data via Zoom cloud, Google Drive (restrict permissions of other users such as to view only), Dropbox, or Box, and that no data will be downloaded to personal computers without password protection.

If your study involves PHI, please contact the IRB office to discuss additional precautions for restricted data (e.g., limits on downloading, transforming, and altering data) and rules for sharing among researchers (e.g., cannot be shared with those outside of Pepperdine University).