Office of Research, Grants and Contracts
Guidance

Guidance Title	Utilizing Zoom for Human Subjects Research				
Date Last Revised		Date Created	01/22/2025	Revision #	
Guidance Number	5	Website	☒Document	☐Pasted	
Applicability	☐ RGC Internal	☒Researcher		☐Institutional	
Subgroup	☐ NKU Compliance	☒IRB	☐IACUC	☐IBC	

1.0 GUIDANCE

Zoom, a widely used video conferencing tool, serves as a convenient host for collecting essential data through virtual interviews and other communication channels. It's crucial to acknowledge that, like most online platforms, Zoom poses potential privacy and security risks. This comprehensive guide emphasizes the importance of safeguarding research participants and collected data and provides detailed instructions for researchers.

The provided guidance assumes that the user uses a Northern Kentucky University (NKU) affiliated Zoom account. Details on getting started on Zoom, tutorials and training resources, security profiles, and guidelines for the use of virtual backgrounds for online meetings can be located in the Zoom knowledge base on NKU's service desk website.

GENERAL CONSIDERATIONS

RESTRICT RESEARCH INTERACTIONS INVOLVING THE COLLECTION OF SENSITIVE DATA

To ensure the security of highly sensitive data, it is imperative to limit research interactions involving such information. It's crucial to be aware that Zoom Inc. may have access to any audio or video content collected through its platform.

RESEARCH CONDUCTED AT HIPAA-COVERED ENTITIES

Northern Kentucky University is not a Health Insurance Portability and Accountability Act (HIPAA) covered entity. However, sometimes NKU faculty, staff and students conduct research outside of NKU at facilities that are considered HIPAA-covered entities.

If your study will be taking place at a HIPAA-covered entity, please be aware that the free and regular paid versions of Zoom, lack compliance with the HIPAA. Consequently, these versions should be avoided for studies that entail the collection or utilization of protected health information (PHI).

In cases where the collection of protected health information is anticipated, researchers are strongly advised to reach out to the Institutional Review Board (IRB) office. This communication is essential for discussing the possibility of obtaining temporary access to a HIPAA-compliant Zoom account. Utilizing this specialized account ensures restricted data retention timeframes and enhanced data-sharing controls.

EXERCISE CAUTION AND LIMIT THE USE OF THE RECORD FUNCTION

It is strongly advised to exercise caution and limit the use of the record function on Zoom. Recording sessions on Zoom can introduce additional security and privacy risks if not handled appropriately. The recording function should only be employed when necessary and exclusively during official study activities. For instance, it is recommended to activate the recording function when commencing official study tasks, such as asking questions from a prepared questionnaire. It is essential to refrain from recording during the set-up or introduction portions of the Zoom meeting to mitigate potential risks and safeguard the privacy of participants.

MINIMIZE THE COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION

To enhance participant privacy and security, it is recommended to minimize the collection of personally identifiable information, which includes both voice and video recordings. These forms of data are particularly vulnerable as they contain information that can identify the participant. The inclusion of such details raises the risk of a breach of confidentiality and privacy agreements if unauthorized individuals gain access to the data.

In the context of recording from Zoom, it's important to note that both video and audio are automatically captured. Therefore, best practices involve limiting the number of identifiers captured in recordings. If video is not essential for your study, it is advisable to promptly delete the video file after uploading the recordings to the Zoom cloud. This proactive measure helps minimize the presence of identifiers linked to participants, reinforcing the commitment to safeguarding their privacy.

PRIVACY AND SECURITY SETTINGS AND TIPS

To enhance security during meetings and webinars, Zoom provides an extensive range of security features and settings. The following options effectively minimize the potential for meeting disruptions, contributing to enhanced privacy and confidentiality during data collection using this platform.

ENABLE ZOOM'S END-TO-END (E2EE) ENCRYPTION FOR MEETINGS

Starting from January 9th, 2024, Zoom has introduced the option for Account owners and admins to enable end-to-end encryption (E2EE) for meetings, offering an added layer of protection when deemed necessary. With E2EE enabled in a meeting, only the participants

themselves, and not even Zoom's servers, have access to the encryption keys used for securing the meeting.

To utilize end-to-end encryption, all meeting participants must join from the Zoom desktop client, mobile app, or Zoom Rooms. It's important to note that enabling this version of Zoom's E2EE comes with certain limitations, including the disabling of features such as join before host, cloud recording, streaming, live transcription, Breakout Rooms, and polling.

IF YOUR MEETING REQUIRES END-TO-END ENCRYPTION, PLEASE CONTACT THE *NKU IT Help Desk* TO HOST THIS SESSION.

CREATE PRIVATE MEETINGS

When setting up a new Zoom meeting, avoid using your Personal Meeting ID; instead, generate a unique meeting code for each session. Additionally, ensure that a password is required to join any meeting. For each meeting, a new link and a new password should be generated for each participant.

ADJUST SECURITY SETTINGS

To access the meeting security setting before starting a meeting, start by signing in to the Zoom web portal. In the navigation menu, click “Settings”. Click the “Meeting” tab.
Note: If any option is grayed out, it has been locked at either the group or account level. You need to contact your Zoom admin.

To view In-meeting security options as the host, locate the shield icon labeled “security”; this will appear between the “start Video,” icon and the “participants” icon.

Enable Waiting Rooms

This feature permits the host to screen incoming participants before granting them access to the meeting. The host can either permit the participant to join or remove them from the meeting. When waiting rooms are activated, participants awaiting the host's approval to join will encounter a screen displaying the message "Waiting for the host to start this meeting," along with a customizable line of text.

(Optional) Lock Meetings

This function allows the host to ‘lock the meeting’, preventing new participants from joining, even if they have the meeting ID and passcode.

(Optional) Hide Profile Pictures

The Hide Profile Pictures function gives the host the option to conceal all participant profile pictures, displaying only their names, including the host. This setting proves beneficial in avoiding distracting or inappropriate images and increasing security and privacy during meetings and webinars.

RECORD FUNCTION: PRIVACY AND SECURITY SETTINGS AND TIPS

Turn off “display participants’ names” in the recording.
Enabling this configuration guarantees that the names of participants won't be included in recorded sessions. You can locate this setting in the recording settings under the gear icon at the top right. In the same menu, there is an optional but recommended feature that enables the host to record individual audio files for each participant.

ENSURE ALL PARTICIPANTS PROVIDE VERBAL AND INFORMED CONSENT BEFORE RECORDING

Although participants are alerted once a meeting starts recording, all researchers are expected to verbally consent participants before recording any session, in addition to obtaining participants’ written consent via the consent form. No participants should be recorded that have indicated they do not want this function used.

SAVING ZOOM RECORDINGS

When using the Record function, prioritize recording to a password protected computer, rather than saving to Zoom Cloud. Zoom meeting recordings that contain restricted data must never be sent via email, or stored, without encryption protections. If the recording involves confidential data only and not restricted data, this data can be stored on a local password-protected computer, Google Drive (with sharing permissions set properly), and other password-protected storage options.

It is crucial to be aware of and adhere to the protection requirements associated with the types of data. If you are unsure of the requirements or have any questions, please see the NIH’s Data Management and Sharing Policy.

WHEN EMPLOYING CLOUD RECORDINGS

Using Cloud Recording, although not ideal, may become necessary for certain features such as Zoom's "Audio Transcript" feature. To proceed with Cloud Recordings, participants' consent is required. The "Confidentiality" section of the consent form should explicitly state the following information:

- Inform participants that recordings will be stored on the Zoom Cloud.

- Specify the timeframe for the deletion of these recordings, emphasizing the need for prompt removal from the Zoom Cloud.

DELETE VIDEO AND AUDIO FILES ONCE A WRITTEN TRANSCRIPTION IS CREATED

After transcriptions are generated, it is imperative to promptly delete the video and audio files from your local drive. If there is a valid reason to retain these files for your study, it is essential to provide an explanation in your IRB application. Additionally, outline additional protective measures that will be implemented to minimize the risk of unauthorized access to this information by others.

GUIDELINES ON FILE SHARING AND REPORTING PROCEDURES IN IRB

When sending data that lacks personal identifiers via email, it suffices to encrypt the email. However, for identifiable data, data must be transmitted via a secure service or by using secure protocols. Ensure to detail your data sharing approach in your IRB protocol, explicitly stating that no data will be downloaded to personal computers without password protection. This information should be included in the Data Collection, Protection, and Records Retention section, addressing the question "Why is it necessary to collect identifiable information and specifically describe the coding system you will use to protect against disclosure?" in the IRB protocol. Additionally, ensure the same information is included in the informed consent form.

Required information for participants:

This information must be included in either the consent form or presented to participants at the beginning of the Zoom meeting.

- Remind participants that they can minimize the risk of conversations being overheard and interruptions that occur by conducting activities in a private and quiet space, minimizing the risk of conversations being overheard and interruptions.
- Participants should be informed about and receive a copy of Zoom's Privacy Policy; specifically, inform participants that Zoom recordings are not private and Zoom may have access to them. Additionally, participants should understand that Zoom recordings (audio or video) are considered identifiable data.
- Participants should be told how and where Zoom recordings will be saved, how recordings will be protected, and when recordings will be destroyed.
- This information can be incorporated into the consent form or recruitment script, or it can be presented at the outset of the Zoom session.

ADDITIONAL RESOURCES:

To access additional details about the security features and functionalities offered by Zoom, kindly refer to Zoom's Security guide.

2.0 REFERENCES

3.0 FORMS OR ATTACHMENTS

4.0 DEFINITIONS

Approvals

Title	Approved	Date Approved	Not Applicable
Manager of Research Compliance	☒	02/07/2025	☐
IRB Chair	☒	02/07/2025	☐
Institutional Official	☐		☒

Revisions

Title	Approved	Date Approved	N/A	Summary
Manager of Research Compliance	☐		☐	
IRB Chair	☐		☐	
Institutional Official	☐		☐	