Guidelines for Using Zoom (Part 4)

4.1.2 (Can be used verbatim)

The online interviews will be held via Zoom, which is an online video/ audio meeting program. The Zoom meetings require an account number and each meeting requires an individual login password. Zoom ensures the security of data through encryption of data in transit and at rest and meets industry and security organization standards (SOC 2; FedRAMP; GDPR,CCPA, COPPA, FERPA, and HIPAA; Privacy Shield Certified; and TrustArc Certified Privacy Practices and Statements). Zoom servers are located outside of Canada and Zoom stores users’ names and usage data outside of Canada.

4.1.3 (Can be used verbatim)

All University of Regina researchers have permission to use Zoom through the University’s license.

4.1.4 (Can be used verbatim)

Each Zoom participant, will be given a randomly generated unique meeting ID and password to enter the waiting room where the principal investigator will admit them to the meeting. The meeting will be subsequently locked to prevent anyone else from joining the meeting once the interview begins. All recordings will be stored on the primary researcher’s host device which is password-protected (and not on the Zoom cloud).

Consent form:

Please include:

* Zoom servers are located outside of Canada and Zoom stores users’ names and usage data outside of Canada.
* Please be clear on the consent form whether you are audio and video recording or just audio recording.

Method considerations:

TCPS-2 Article 4.1: Inclusion

* Not everyone has access to technology or an adequate comfort level to use technology

TCPS-2 Article 3.12: Consent

* While, in some cases, it may be acceptable to provide the consent form to the participant over email, please do not use an identifier of potential participation in a research study in the subject line. Further, because email is not a secure form of communication, it is not recommended that the participant return a signed consent form via email. Alternatively, please consider obtaining oral consent during the scheduled meeting. Please include a statement on the consent form that email is not a secure form of communication and there is a possibility that your email communications could be intercepted by outside sources.
* Be clear whether audio and/or video recording or both and obtain consent

TCPS-2 Article 5.1: Privacy and confidentiality

* The technology adds identification of the individual (user name appears under the image)
* Ask participants to participate in a confidential space where their responses cannot be overheard
* As a researcher, conduct the interview in a confidential space where the participant’s responses cannot be overheard; consider wearing a headset so no one can inadvertently hear the interview
* Possibly scan the space around you to ensure the participant that no one else is in the room or could enter while conducting the interview
* Give participants the option not to turn on their camera or to use a background scene
* It is not recommended that if you are using the record feature on Zoom that you save to the Cloud. Please store the recordings securely on the researcher’s host device. Unfortunately, this procedure also disables the automatic transcription of the interview.
* Consider deleting audio and/or video recordings once transcribed
* If the interviews are to be transcribed, who will be doing this? If not the PI, is this clear on the consent form? If not the PI, how will the data be transported to the transcriptionist? Will transcripts be forwarded back to participants for review, and if so how will confidentiality be maintained through this process? Because email is not a secure mode for data transfer, it is recommended that you use a password protected file to communicate with the participants and/or transcriptionist. Please make sure to send the password in a second email. Also, ensure that no group emails are sent to the participants (use BCC) and that the emails will be securely stored separately from the data.

TCPS-2 Article 6.12: Risk

* Be cognizant of potential for “Zoom fatigue” if participant is in an occupation that spends a lot of time during the day on Zoom.

For the information of the researcher:

Please make sure to adhere to Zoom guidance as follows: <https://www.uregina.ca/is/security/advisories/security-advisory57.html>

Since it is not readily apparent how to do disable the Cloud recording option, the following instructions are provided.

To disable Zoom Recording in Cloud (<https://support.zoom.us/hc/en-us/articles/203741855-Cloud-recording>), please have each user:  
1.Sign in to the Zoom web portal.  
2.In the navigation panel, click Settings.  
3.Navigate to the Recording tab and verify that the Cloud Recording setting is DISABLED.  
Each user who is conducting interviews should configure this to disable cloud recording.  
Once this is done, local recording can be used per: <https://support.zoom.us/hc/en-us/articles/115004794983>