Zoom Guidance for IRB Studies

When using Zoom technology, at a minimum, please follow the guidelines outlined below:

1) **Create private meetings.** Make sure that all meetings with research participants have a password enabled. A new link and a new password should be generated for each participant.
2) **Enable the Waiting Room function** (available under Meeting Options). This will allow the host to approve each new attendee.
3) **Establish ground rules with participants**; this could include not taking screen shots, not recording the session etc.
4) **Limit research interactions that collect highly sensitive data**. Remember that Zoom may have access to any audio or video collected on Zoom. Also, the free and regular paid versions of Zoom are not HIPAA compliant and should not be used for any study involving the collection or use of protected health information (PHI).
5) **Limit the use of the Record function.** Recording sessions presents additional security and privacy risks when not handled properly. Only use this function when absolutely necessary, and be clear with your participants when sessions will be recorded.
6) **When using Record function, please make sure all participants consent.** The meeting room should require permission and/or alert participants that they are being recorded, however, all researchers are expected to verbally consent participants prior to recording any session. No participants should be recorded that have indicated they do not want this function used.
7) **When using Record function, always record to the computer.** Though you will have the option to record to the cloud, please refrain from doing so. All recorded meetings should be saved to the password protected computer.
    a. **To disable Cloud Recordings (this is the preferred setting for recordings) follow these steps:**
        i. In the "Meeting Settings" select the "Recording" tab.
        Turn ON the "Record on the local computer" option.
        Turn OFF the "Cloud Recording" option.
        ii. This enables you to save both audio and video files of Zoom recordings to your computer.
    b. **If using Cloud Recordings:**
        i. In some cases, it may be necessary for you to use Cloud Recordings in order to utilize Zoom's "Audio Transcript" feature. If you would like to create Cloud Recordings, participants must provide their consent. You must include the following information in the "Confidentiality" section of the consent form:
            1. Tell participants that recordings will be stored on the Zoom Cloud and tell them when those recordings will be deleted (recordings should be deleted as soon as possible from the Zoom Cloud).

Sources:
"Researcher Guidance for the Use of Zoom in Data Collection"
University of Illinois at Urbana-Champaign ('Illinois') Office for the Protection of Research Subjects ('OPRS')
"Zoom Guidance for IRB Studies," The University of Maine

2. Tell participants that the recordings are subject to the Zoom's privacy policy.

Remind Participants:

1) Participants should be reminded to protect their privacy by completing activities in a private and quiet space, to ensure conversations are not overheard and ensure that there are minimal interruptions.
2) Participants should understand that Zoom recordings are not private because Zoom may have access to them.
3) Participants should understand that Zoom recordings (audio or video) are considered identifiable data.
4) Participants should be told how and where Zoom recordings will be saved, how recordings will be protected, and when recordings will be destroyed.
5) This information can be included in the consent form or recruitment script, or presented at the beginning of the Zoom session.

For additional information, review Zoom Security Guide https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

Sources:
"Researcher Guidance for the Use of Zoom in Data Collection"
University of Illinois at Urbana-Champaign ('Illinois') Office for the Protection of Research Subjects ('OPRS')
"Zoom Guidance for IRB Studies," The University of Maine