# Audio/video recording using zoom software:
# Best practice for research

The following best practices are recommended for human subject research using Zoom software for digitally recording participants responses/behavior.

The following assumptions are in place:

- The data collection process and the risks of data breach are made clear to the research participant during and after the consenting process.
- Participants are not prisoners or being recorded in a forensic setting.
- Participants are being recorded in a private setting, and the chances of non-research individuals being accidently recorded (i.e., individuals who have not been consented) is minimized as much as reasonably possible.
- The data are not being obtained from or shared with a “covered entity”, as defined by DHH & HIPAA.

**NOTE:** Potentially sensitive information can be recorded during the Zoom interview if appropriate security measures are in place. Sensitive information, including information about physical and mental health, is deemed “Research Health Information” (RHI) by the LSU IRB unless the data are governed by HIPAA. If this is the case, a HIPAA authorization will be needed in addition to a Business Associates Agreement (for 3rd parties receiving data).

## Recommendations for Meetings

NOTE: Most of these settings can be configured with zoom platform https://lsu.zoom.com while some would require action within the meeting):

1. All meetings should be configured to utilize automatically generated Meeting ID rather than personal Meeting ID
2. All meetings with external clients must be unique and require passwords.
3. All meetings with internal (LSU A&M users) must be unique and require authentication using LSU authentication (See GROK article here - https://grok.lsu.edu/Article.aspx?articleid=20118)
4. Zoom waiting rooms must be enabled for each meeting
5. Once all participants have entered a meeting, the meetings must be locked (See GROK article here - https://grok.lsu.edu/Article.aspx?articleid=20118)
6. All meetings should start with video for both the host and participants off.
7. Where possible only utilize computer audio and telephone option should be switched off unless absolutely necessary. In the event telephone option is offered, please ensure that password is required for such attendees as well.
8. Disable join before host
9. Disable file transfer capabilities in meetings unless absolutely necessary
10. Limit screensharing to host only.
11. Ensure that the setting to allow removed participants to join is disabled.

12. Do not allow participants to rename themselves in the meeting

**Additional Recommendations for Meeting Recordings:**

1. Disable the ability for local recording (this is for security/privacy reasons as well as efficiency reasons to maintain network bandwidth for end users).
2. All recordings should happen in the cloud.
3. Disable the ability to record chat messages unless absolutely necessary.
4. Do not record meetings automatically when they start
5. All recordings need to be limited to authenticated users and should require a password to access.
6. All recordings should be deleted after 30 days.