Best Practices for Stan State Investigators Conducting Human Subjects Research (HSR): Remote HSR & COVID-19

The social distancing measures adopted across the nation in response to COVID-19 have changed the ways that investigators conduct research with human subjects. As investigators can no longer meet face-to-face with participants to collect data, a transition to remote or virtual data collection is appropriate. The University Institutional Review Board (UIRB) offers the following best practices for investigators working remotely with confidential participant data.

Secure Your Physical Workspace While Working Remotely

Ideally, investigators will set-up a private and secure remote workspace, to properly protect study records and identifiable data.

If you do not have access to a private, remote workspace, adopt the following best practices when working with HSR:

- Any virtual meetings or telephone calls with participants should be conducted in a private space;
- Wear headphones to limit what others who may be nearby can hear of your discussion
- Be alert to what appears in your background;
  - IRB standards are in place to protect not only the participant, but the investigator as well. Check that any of your personal or identifying information is not visible to participants.
- Position your computer screen so that others cannot see subject information or data;
- close your laptop and lock the screen when not in use;
- Secure physical paper records and data in a safe place.

Maintaining Privacy and Confidentiality in Virtual Meetings

If you plan to interact with participants online or in a virtual meeting, appropriate efforts must be made to secure the meeting in order to protect participant confidentiality. Every Stan State faculty member, staff, and student has access to Zoom Web Conferencing. Other formats with similar protection options may be utilized, but you may want to consult with the IRB Coordinator with any questions related to other virtual programs.

Conducting Virtual Interviews via Zoom

- Password protect your meeting
  - Enable **Require a password when scheduling new meetings or webinars** through the **Meeting** tab of your Settings. Participants will then be required to enter a password to join the meeting. See Meeting and Webinar Passwords for more information.
- Recording a meeting
  - If the participant consents to the meeting being recorded, you should save the recording and any transcripts to your personal computer, rather than the cloud.

Conducting Virtual Focus Groups via Zoom

- Control when participants can join the meeting
  - Send participants to the **Waiting Room**. (Meetings only) Only the host can allow participants in the **Waiting Room** into the live meeting. See Waiting Room for more information.
  - Disable **Join before hosts** to ensure participants are not able to join the meeting before the host arrives. See Scheduling meetings for more information.

- Control communication between participants
  - Disable **In Meeting Chat** through your **Profile** settings. Here you can toggle off allowing participants to chat. This is also where you can prevent users from saving chat. See Disabling In-Meeting Chat for more information.
- Secure information shared in the focus group
  - Ensure only hosts can share their screen through Settings by un-checking **Participants** under **Who can Share?** See Managing participants in a meeting for more information. This is on by default.
  - Disable **File Transfer** in **Settings**, which will ensure participants are not allowed to share files in the in-meeting chat during the meeting. See In-Meeting File Transfer for more information.
- Protect the identity of participants from other focus group members
  - Stop a participant’s video stream to ensure participants are not on video through **Manage Participants**. See Managing participants in a meeting for more information.
  - Click to **Mask phone numbers in the participant list** through the **Telephone** tab in Settings. This hides all telephone numbers called into the meeting.

General best practices for establishing virtual meetings in HSR:

- Do not publish the meeting URL in public communication channels

- Remind participants to not share meeting details with others
- Send each participant a meeting invitation separately – no mass email (focus group participants)

General Data Security Reminder

Regular IRB standards for securing study data still apply when working remotely. The following are some best practices for storing data securely in a remote setting*:*

- All data collection and storage devices must be password protected with a strong password. Do not share your password with anyone.

- All sensitive research information on portable devices must be password protected.

- Access to identifiable data should be limited to only the Principal Investigator and any study members listed on the IRB application.

- Identifiers, data, and keys should be placed in separate, password protected/encrypted files and each file should be stored in a different secure location.

- If possible, all identifiable participant data should be stored on an external hard drive or a USB drive that can be physically protected (i.e. a locked file cabinet).