MU IRB Suggestions for Maintaining Data Security When Working Remotely

This information can be included as part of any online survey, as part of an informed consent, or presented to a study participant(s) at the start of an online interview or focus group.

- Inform participants of steps they can take to protect privacy (e.g., closing their web browser after survey completion, avoid using shared devices, finding a private location to complete interviews, etc.).

- Be familiar with platform settings necessary to protect privacy. Whenever possible, disable functions that automatically collect electronic identifiers, such as IP addresses or cookies.

- When conducting interviews via phone/videoconferencing – take precautions to protect participant privacy (e.g., do not conduct a video interview in a publicly occupied space or a common room where roommates/family members may overhear).

- Focus groups conducted using videoconferencing software (i.e. Webex or Zoom) must include extra precautions as confidentiality and privacy of all group participants relies on other members.
    - Group members should be reminded that they are each responsible for taking precautions to protect the privacy of fellow participants.
    - Researchers should configure videoconferencing software to prohibit recording by participants.
    - Participants should be instructed to not record/take screenshots
    - Participants should be mindful about location to prevent roommates/family members/public from easily overhearing/seeing other participants. Use a private location and be conscious of public areas, shared common areas, poor acoustics, etc.
    - All participants should be reminded of the unique limitations to privacy on digital platforms and to use discretion when sharing.
- Qualtrics remains the most secure method for collecting survey data and its use is strongly encouraged.