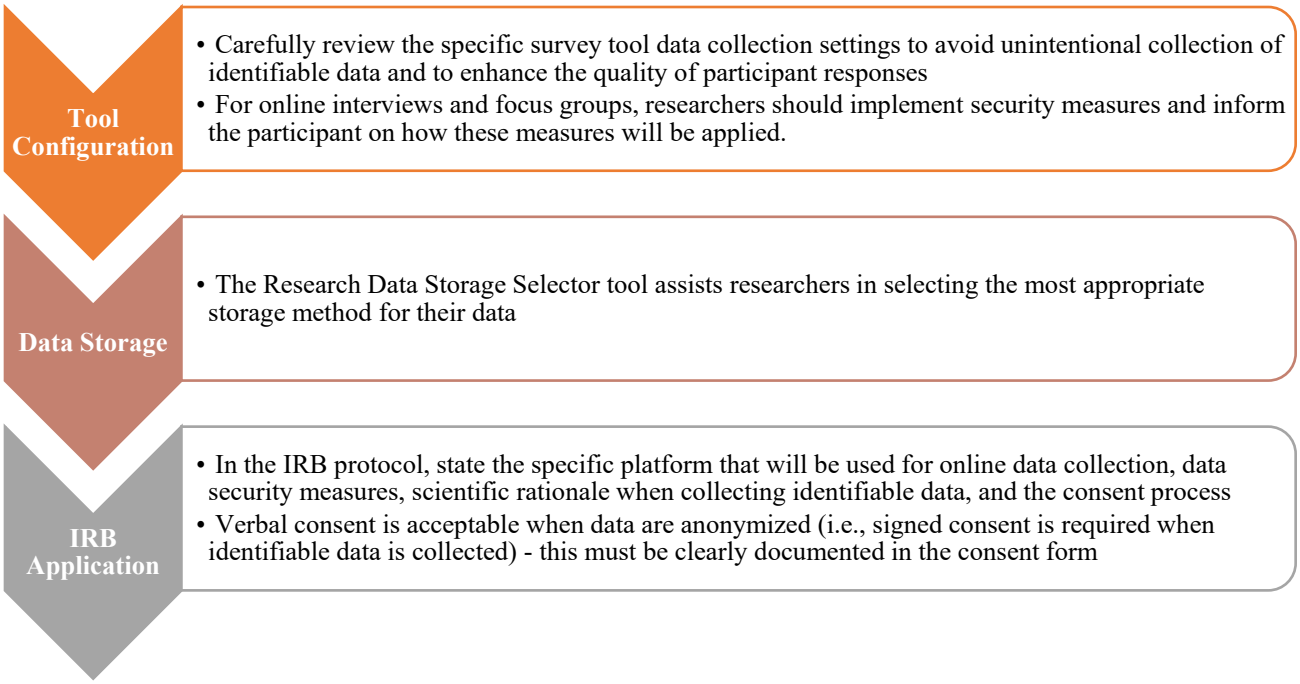
IRB Guidance on Online-Based Research

(Last Updated on 4/29/24)

When performing online data collection in the form of surveys, interviews, and/or focus groups, researchers must consider:

A. Tool's configuration with respect to protecting participant's privacy
B. Selecting the appropriate data storage method
C. Adequately addressing the IRB application (i.e., protocol and consent form)

The following graphic highlights key concepts of the guidance document that will be described in detail below:



Tool Configuration

Online data collection procedures such as the administration of surveys, interviews, and/or focus groups are appropriate for studies that are considered "no greater than minimal risk" to participants. Per the ASU Human Subjects Research Procedures, and Federal Regulations minimal risk is defined as "A risk that is minimal where the probability and magnitude of harm or discomfort anticipated in the proposed research are not greater, in and of themselves, than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests." The researcher must carefully review the platform's configuration settings on data collection to ensure that the participant's privacy and data are protected. In addition, the researcher should also take these into account when planning their data collection method(s).

Survey Procedure Considerations

For administrating an online survey, the researcher should take note of the following aspects:

A. Anonymizing responses to avoid unintentional collection of identifiable information: Qualtrics and SurveyMonkey by default collect participant IP addresses (which are considered identifiable information). Both survey platforms can anonymize responses to provide optimal protection of participant data.
    i. For details on how to do this in Qualtrics, visit: http://www.qualtrics.com/university/researchsuite/advanced-building/survey-flow/anonymize-responses/
    ii. For details on how to do this in SurveyMonkey, visit: http://help.surveymonkey.com/articles/en_US/kb/How-do-I-make-surveys-anonymous

    iii. It is important to note that if Google Forms is used as a method of data collection, IP addresses are not collected by default. It is also important to note that if crowdsourcing tools such as Amazon MTurk or Prolific Academic are used to deploy surveys, they are not considered anonymous as both methods collect worker IDs for payment purposes. Worker IDs can be linked to participant identities, both publicly and privately.

B. Researchers should design their survey instrument in a way that allows participants to skip specific questions that could potentially provide discomfort or breach of privacy. This can be achieved by including a response option such as "Decline to answer." Further, participants must always be given the option to withdraw from a study, even while in the middle of a survey. This can be made known to the participant when going through the consent process.
    i. To ensure that Researchers are receiving quality responses from participants, they can include the following survey controls:
        1. Create a screening questionnaire with study specific inclusion criteria that participants must attest they meet the criteria to fill out the survey
        2. Include attention checks within the survey (e.g., "To ensure that you are paying attention, please select the third option from the choices below")
        3. Use ReCAPTCHA to determine if the respondent is human or a bot

Interview and Focus Group Procedure Considerations

When conducting interviews and/or focus groups online, Researchers should consider the following data security and participant protection measures:

A. Participants should use a virtual background feature, when available, if they do not want to have their surroundings visible – this can be used when participants agree to be video recorded, but do not want their location known.

B. The host can select the "host only" setting to prevent others from sharing their screens. If the host determines that screen sharing by participants is needed, sharing by "one participant at a time" should be selected. The host should remind participants not to share other sensitive information during the meeting inadvertently. This can be verbally stated as well as in the consent form (e.g., when conducting focus groups).

C. Generate a new meeting code (and/or pass code) to prevent unwanted participants from entering your meeting.

Data Storage

To determine the appropriate platform for storing your data, the Research Data Management Team has developed a tool to help researchers identify the most appropriate storage option based on data classification, sharing, and accessibility: https://researchstorage.asu.edu/

Research teams should choose storage solutions that provide the appropriate level of protection for the research data collected. All data should be stored in a secure manner. Computer hard drives and USB drives should only be considered as temporary storage solution, and only if the data are non-sensitive in nature.

Approved long-term storage solutions for human subjects research data that contain Personal Identifiable Information (PII) include: The Arizona Secure Research Environment (ASRE) and REDCap.

Approved storage solutions for anonymized human subject data for example include Dropbox for Education, Google Cloud Storage, and Google Drive.

For assistance contact the Research Data Management Office.

IRB Application

Regardless of the mode of online data collection (survey, interviews, etc.), there are essential components required within an IRB protocol and the consent form.

IRB Protocol

A. Study Procedures (Section 7 in Social/Behavioral Application; Section 8 in Bioscience Application)
   i. Indicate the specific survey and/or video conferencing software that will be used and expected time duration to complete each procedure.
   ii. For surveys, if participants are allowed to skip questions, indicate how participants will be allowed to skip questions if they wish to complete the entire survey (e.g., including an option to "Decline to answer" as a response).
   iii. For interviews and/or focus groups that will be conducted online, state any security settings that will be implemented (e.g., a meeting passcode to enter the Zoom meeting).

B. Privacy and Confidentiality (Section 11 in Social/Behavioral Application; Section 16 in Bioscience Application)
   i. Indicate how data collected from survey and/or interview will be stored.
   ii. Notate the type of data that will be collected (e.g., survey responses, audio recordings, video recordings)
   iii. Document how the data will be de-identified (e.g., a master list containing identifiers, participant ID)

iv. For identifiable information that will be collected for research purposes, provide scientific rationale for obtaining this data. If the only identifying information being collected is for the drawing and to determine whether a participant has responded, it is recommended that you collect contact information outside of the survey/interview to maintain anonymity of responses of participants. This can be accomplished by directing participants to a second survey page or directing participants to email their contact information to a designated email address. See https://www.qualtrics.com/community/discussion/385/how-to-set-up-a-sweepstakes-in-an-anonymous-survey for a method to link to a second survey.

C. Consent Process (Section 12 in Social/Behavioral Application; Section 17 in Bioscience Application)
   i. If only de-identified data from a survey is being collected from participants, then a waiver of signature on consent form/implied consent is appropriate. Implied consent indicates that the participant agrees to participate in the research by continuing to complete the survey.
   ii. If only audio recordings are being collected from participants, then verbal consent is appropriate. The participant must verbally agree to participate in the research prior to answering interview questions.
   iii. For video recordings, focus groups (regardless of only audio recordings are maintained), and surveys that intend to collect identifiable information, signed consent (with a signature block stating the participant's name, participant's signature, and the date) is required.

Consent Form

Depending on the type of data being collected (as mentioned in the previous section), researchers can review the sample consent verbiage provided below and tailor it specific to the study:

A. For surveys where only de-identified data is collected (at the end of the form):
   "Click 'continue' below if you consent to participate in the study"
   "If you agree, click 'next' to start the survey"

B. For interviews where audio recordings are collected (at the end of the form):
   "Your verbal agreement indicates your consent to participate"

C. Standard audio (or video) recording language:
   If you are video recording the interviews, obtaining written consent via signature is appropriate. When using Zoom and you plan to retain only audio recording for analysis, it is recommended that researchers use the standard language below to explain this aspect:
   "I would like to record this interview using Zoom. Zoom records an audio and video track of the interview. [The research team will retain only the audio track for analysis.] The interview will not be recorded without your permission. If you would like to participate in an audio only interview, turn off your camera. Please let me know if you do not want the interview to be recorded; you also can change your mind after the interview starts, just let me know."
   (Revise as appropriate to reflect this study's procedures.)

D. If crowdsourcing via MTurk, Prolific, or another online platform where an ID # is collected to compensate for participation, language in the consent form should clearly explain what information is collected, even temporarily. See example language below: "We will not ask your name or any other identifying information in this survey. For research purposes, an anonymous numeric code will be assigned to your responses. However, your [Amazon MTurk worker ID number or Prolific ID #] will be temporarily stored to pay you for your time; this data will be deleted as soon as it is reasonably possible. [You have the option of making your personal information private by changing your MTurk settings through Amazon.]"

Lastly, it is also important that researchers should be careful not to make guarantees of confidentiality or anonymity, as the security of online transmissions is always in question.

References

1. https://und.edu/research/resources/human-subjects/_files/docs/guidance-for-conducting-studies-online.pdf

2. https://www.marquette.edu/research-compliance/documents/irb/guidance_on_on-line_surveys_final.pdf

3. https://www.boisestate.edu/research-compliance/irb/guidance/guidance-for-computer-and-internet-based-research/

4. https://www.shepherd.edu/app/uploads/2016/05/Online-Data-Collection-IRB-Issues.pdf

5. https://ethics.berkeley.edu/privacy-considerations-when-using-zoom

6. https://www.uiw.edu/orgs/_docs/irb/guidance-crowdsourcing-tools.pdf

7. https://cphs.berkeley.edu/mechanicalturk.pdf