Risks such as violation of privacy, legal risks, psychosocial stress are minimized

1.5.3 could be stigmatizing.

2.0 Use of Internet for Subject Recruitment

2.1 The IRB must review and approve all materials used for posting recruitment materials on the internet, e.g., through a website, a banner advertisement, or an email solicitation.

2.2 Computer- and internet-based procedures for advertising and recruiting potential study participants (e.g., internet advertising, email solicitation, banner ads) must follow the IRB guidelines for recruitment that apply to any traditional media, such as newspapers and bulletin boards.

2.3 /vÀ•š]P š}Œ•ŒŒ‹µ•š]vP š}ŒŒµ]šš ZŒ}µPZ h^[•u

the appropriate USA policies and procedures for review and approval in addition to obtaining IRB approval for the recruitment procedure and message content.

3.0 IRB Requirements

3.1 The IRB must review all research activities involving the use of the internet with the same considerations and standards for approval of waiver (45 CFR 46.111), for informed consent, and voluntary participation as all other research activities under the jurisdiction of the USAIRB.

3.1.1 The IRB must evaluate the appropriateness of the informed consent process.

3.1.2 The IRB must take into consideration data collection and security.

3.2 The IRB review must include a consideration for the delineation of boundaries (i.e., would the participant consider the access private or public space of the internet).

3.3 The IRB must consider all additional requirements for the approval of research that involves a vulnerable population as all other studies recruiting those populations.

3.4 As there is no standard for identifying distressed participants online, the IRB must take into consideration potential participant experiences (the sensitive nature of the research) that may be distressing when evaluating the risk/benefit ratio.

5.0 Data Collection/Storage:

5.1 Data collected from human subjects over computer networks should be transmitted in encrypted format.

5.2 All databases storing identifiable information or data must be protected regardless of the source creating the data (e.g., encryption of the database, de identifying the database

5.3 In general, personal identifiers such as Social Security Number, hospital or clinical patient numbers, or other information which might identify research

The researcher is obligated to maintain compliance with the Terms of Service for any resource they access for data collection. The IRB will not review the Terms of Service for each application unless a consultation is requested prior to IRB approval. Researchers are also responsible for ensuring their research does not violate revisions or updates to Terms of Service during the conduct of research.

6.1.1 Use of Amazon Mechanical Turk (MTurk)

The use of MTurk as a recruitment method for human participant studies [illegible] turkers.

For additional information, see IRB Guidance Recommendations for Using Mechanical Turk (MTurk) for Social/Behavioral Projects

6.1.2 Qualtrics

The University of South Alabama supports Qualtrics survey tool for creating, delivering, and analyzing surveys and survey responses for academic, administrative, and research related purposes. Qualtrics is available to all current University faculty, staff, and students, when supervised by faculty in a class or research setting. The use of Qualtrics is bound by [illegible] Use Statement.

For additional information, see University of South Alabama Qualtrics webpage, Resources for Researchers

7.1 Survey Software Checklist

Researchers should consider the following:

7.1.1 Using encryption software when handling sensitive information sent to and from websites
7.1.2 Are there controls in place to prevent a respondent from accidentally entering survey data via the http protocol instead of the https protocol (i.e. Does the server display an error message or automatically route the respondent to an https page)?
7.1.3 Accessing their data in the database via a username and password.
7.1.4 Ensuring that survey data contained in the database(s) cannot be improperly accessed or information cannot be disclosed to parties other than authorized researchers. How to monitor access to the data to prevent and detect unauthorized access.

7.1.5 Are the servers that contain the research data located in a data center, with physical security controls and environmental controls?
7.1.6 Is there a finite time period in which a deleted dataset can still be retrieved? What is that time period?
7.1.7 Is the respondent's IP address masked from the researcher? If collected, please explain what is done with the information. Do other third parties have access to IP addresses?
7.1.8 Are there any circumstances where you would release the respondent identifiers and their survey responses to third parties?

HISTORY

Effective Date: June, 2007
Revisions: January 2019, March 2021