UMKC
Office of Research Services

19. Computer and Internet Based Human Participant Survey Research

19.1. Policy

Computer and internet based methods of collecting, storing, utilizing, and transmitting data in research involving human participants are developing at a rapid rate. As these new methods become more widespread in research, they present new ways of enhancing the management of surveys to human research participants while also presenting new compliance challenges to the protection of those participants.

This policy sets forth requirements and recommendations by which researchers can plan, develop, and implement computer and internet based survey research protocols that provide equivalent levels of protection of human participants to those found in more traditional research methodologies such as paper based surveys.

All studies, including those using computer and internet technologies, must:

- Ensure that the procedures fulfill the principles of voluntary participation and consent,
- Have appropriate safeguards to protect the privacy or confidentiality of information obtained from or about human participants,
- Adequately address possible risks to participants, including psychosocial stress and related risks.

In determining the adequacy of certain survey programs, data collection and storage methods, and consent procedures for the protection of human participants, the UMKC IRB will assess whether proposed survey research is minimal risk or greater than minimal risk. In making this determination, the IRB will consider whether the resulting data could be stigmatizing, result in criminal or civil liability, damage financial standing, employability, insurability, or reputation, result in stolen identity, or pose a threat to an Individual's confidentiality.

19.2. Online Surveys

Researchers may need to use a variety of software programs and options to distribute and collect survey data over the internet. These options fall within one of the following three broad categories:

- Commercial or third party survey creation and hosting services. In these cases, the researchers often enter into a contract with the vendor to provide some or all of the services related to the creation and management of the internet surveys.
- Surveys developed either internally or using a survey development software, and hosted on web servers managed by researchers or by UMKC IT services.
- Surveys that are conducted via email, because the nature of the transmission to and from respondents may carry additional risks to confidentiality.

Please note that the IRB does not, in any way, promote the use of particular service providers. An approval by the IRB simply means that the written statements and policies around security, privacy and confidentiality of data provided to the IRB by companies allow their use for internet surveys for human participant research.

If the researcher proposes to use a service provider that is not familiar to the IRB, s/he must submit to the IRB, as part of the initial application, an assessment of the security, privacy and confidentiality practices of the service provider. The IRB will, in consultation with the appropriate experts in IT security, as necessary, review the information provided to assess whether or not the service provider can be used for conduct of the survey.

The server used for online surveys of greater than minimal risk must meet the following criteria:

- The server must be administered in accord with current best practices by a professionally trained person with expertise in computer and internet security.
- Access to the server must be limited to key project personnel and configured to minimize the possibility of external access to the server data.
- The server must be subject to periodic vulnerability assessments to determine that the server is configured and patched according to industry best practices.

19.3. Data Storage/Disposal

Personal identifying information must be kept separate from the research data, and both sets of data should be stored in encrypted format.

It is recommended that data backups be stored in a safe location, such as a secure data room that is environmentally controlled and has limited access. Encryption of backup data is also recommended.

Competent data destruction services should be used to ensure that no data can be recovered from obsolete electronic media.

Consultant/partner/vendor must have a written plan to dispose of old data on a consistent basis. This includes but is not limited to the overwriting or physical destruction of storage media e.g. hard drives, tape cartridges, CD/DVD-ROM media before it is surplused or removed from the consultant's premises.

Consultant/partner/vendor must provide a written schedule for when data will be removed from production and backup sites (Examples: upon termination of contract, within 30 days of contract termination, within one year of contract termination, never).

19.4. Allowable Survey Software Based on Study Risk

For online surveys, the sensitivity of the data being collected will be an additional factor in determining the risk level of the study.

19.4.1. For All Non-Exempt Online Survey Methods, the researcher must demonstrate, in their application to the IRB, that the following minimum standards are met:

- Use of a standard encryption technology such as SSL.
- How the security of the web server is being ensured, to prevent unauthorized access.
- A disclosure included in the consent information provided to the participant stating, "*Please note that the survey(s) [is/are] being conducted with the help of [company name], a company not affiliated with UMKC and with its own privacy and security policies that you can find at its website. We anticipate that your participation in this survey presents no greater risk than everyday use of the internet."*

19.4.2. Depending on the Risk Level and the Specific Circumstances of the Study, the IRB may elect to require researchers to provide an alternative means of filling out the survey. In addition, the IRB may elect to require additional protections, such as technical separation of identifiers and data, or a higher level of encryption.

19.5. Recruiting Participants

Computer and internet based procedures for advertising and recruiting potential study subjects (*e.g.*, internet advertising, email solicitation, banner ads) should follow the IRB guidelines for recruitment that apply to any traditional media, such as letters, telephone scripts, newspapers and bulletin boards.

- Permissions should be sought, wherever required, to post research recruitment materials to online sites.

The text of the recruitment script, the context in which the recruitment takes place (*e.g.*, posting a message on a newsgroup, mass emailing, and websites created for recruitment of participants) must be reviewed by the RCO or approved by the IRB.

If researchers wish to recruit participants for which special protection is required by the UMKC IRB (such as children, prisoners, UMKC students or employees, etc.), they should refer to the IRB SOPs on those topics in designing the study.

The IRB may advise researchers to take steps to authenticate respondents, if appropriate, to the study design. For example, investigators can provide each study participant (in person or by regular postal mail) with a personal identification number (PIN) to be used for authentication in

subsequent computer and internet based data collection. The PIN used must not be one that could be used by others to identify the Individual (*e.g.* Social security number, etc.)

Depending on the nature of the research, the IRB may request that methods of incentives and/or compensation allow participants to receive remuneration either without revealing their identities or without connecting their identities to survey responses. *For example:* using gift certificates from online retailers and displaying the unique certificate redemption number to respondents at the completion of a questionnaire. This allows participants to receive an incentive without revealing their identity.

19.6. Consent information

19.6.1. Special Requirements

For internet based surveys, researchers should provide options for prospective participants to indicate their active consent to participate.

For non-exempt research, researchers are required to include a confidentiality disclaimer in the consent document as described previously.

For non-exempt research when conventional written consent will not be obtained, an internet consent document should be written like a cover letter and should include all the elements, as applicable, of a regular signed consent document. For exempt and non-exempt research the consent line should reflect the potential participants willingness to participate by clicking the button/checking the box to proceed to the survey. For web-based surveys, a click- through button/check box should be added.

If the IRB determines that documented consent is required (*e.g.*, participants' anonymity is not maintained and/or the study is greater than minimal risk) the consent form can be mailed or emailed to the participant who can then sign the form and return it via fax or postal mail.

Some survey vendors and/or software packages provide a means to record whether a respondent has consented to participate before beginning the survey(s) (e.g., a date/time stamp feature). If appropriate, researchers should consider the use of this functionality.

For surveys sent to and returned by participants through email, researchers should include an information sheet with consent information and inform participants that submitting the completed survey implies their consent.

Researchers must disable the storage of email addresses and disable IP address collection for all collection methods so that they can collect anonymous survey responses.

<u>Participation by minors</u>

Researchers subject to the Children's Online Privacy Protection Act are prohibited from collecting personal information from a child without posting notices about how the information will be used and without getting verifiable (likely written) parental permission. For minimal risk research, written permission may be obtained via postal mail or fax. If the research is more than minimal risk, parental permission should be obtained in a face-to-face meeting.

For research that excludes minor participants, the IRB may ask the researcher to describe the procedures to be employed to authenticate that the participants are adults. Some options are using internet monitoring software or using adult check systems can screen out minors.

19.7. Skipping Portions of/Withdrawing from the Survey

Unless completion of an entire survey is a requirement of participation, internet-based survey instruments should be formatted in a way that will allow participants to skip questions if they wish or provide a response such as "I choose not to answer."

If completion of an entire survey is a requirement of participation, the consent document should clearly indicate this requirement and remind prospective participants that they may choose not to participate, or stop participation in the research at any time.

If the participant completes an anonymous survey and then submits it to the researcher, the researcher may not be able to extract/remove/delete their specific data from the database should the participant wish it withdrawn. The consent document should inform prospective participants of this limitation.

19.8. Survey Software Checklist

Researchers should consider the following:

- Using encryption software when handling sensitive information sent to and from websites
- 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 re-route the respondent to an https page)?
- Accessing their data in the database via a username and password.
- 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.
- Are the servers that contain the research data located in a data center, with physical security controls and environmental controls?
- Is the data backed up regularly? How often?
- Is there a finite time period in which a deleted dataset can still be retrieved? What is that time period?

- 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?
- Are there any circumstances where you would release the respondent identifiers and their survey responses to third parties?

Approved by: Lawrence Dreyfus, PhD
Name of University Institutional Official

_____
Signature of University Institutional Official Date