UNIVERSITY OF SOUTH ALABAMA

IRB SOP 804
Internet Research

Purpose

The Internet is widely used in the conduct of human subject's research during the recruitment and consent processes, and in data collection. Research using the Internet must provide the same level of protection as any other types of research involving human participants. However, it presents its own unique set of issues and concerns during the IRB review process. The purpose of this document is to help researchers plan, propose, and implement Internet-based research protocols that provide the same level of human subject's protections as more traditional research methodologies

Scope

This Standard Operating Procedures applies to all members of the University of South Alabama and the IRB.

Policy

Internet data collection via email, list servs, electronic bulletin boards and web surveys falls under the purview of the Institutional Review Board. Researchers must adhere to the same ethical principles protecting human subjects as mandated in more traditional research situations. These principles are: Respect for Persons, Beneficence, and Justice and are described in the Belmont Report. These ethical principles are reflected in procedures that seek and obtain informed consent, protect privacy of participants, maintain confidentiality of data, minimize risks and prevent coercion.

The IRB will review the use of internet based research activities, including subject recruitment, in human subject's research to ensure that:

- Risks such as violation of privacy, legal risks, psychosocial stress are minimized
- Subjects' participation is voluntary
- Informed consent requirements are met
- Information obtained from or about human subjects is kept confidential

In general, the Internet is an insecure medium as data in transit may be vulnerable. The potential source of risk is harm resulting from a breach of confidentiality. This risk is heightened if the research involves data that places subjects at risk of criminal or civil liability or could damage their financial standing, employability, insurability, reputation or could be stigmatizing.

In general, email should be avoided for the transmittal of confidential data, unless encrypted. The USA IRB recommends that Investigators follow the procedures outlined below to ensure the adequate protection of research participants and guarantee the validity of the data collected. These procedures will assist Investigators plan and implement internet-based research studies while providing the same level of protection of human subjects involved in more traditional research studies.

Procedures

1.0 Informed Consent Process

1.1 For anonymous Internet-based surveys, it is sometimes appropriate to provide participants with informed consent information, and inform participants that submitting the completed survey implies their consent. Alternately, Internet-based surveys could include "I agree" or "I do not agree" buttons with which participants would indicate their active choice of whether or not they consent to participate.

1.2 For surveys sent to and returned by participant via email, investigators should include a consent document and inform participants that submitting the completed survey indicates their consent. This would constitute unsigned consent. In order to utilize this consent procedure, the investigator must request a waiver of documented consent.

1.3 Researchers conducting web-based research should be careful not to make guarantees of confidentiality or anonymity, as the security of online transmissions may not be guaranteed.

1.4 Researchers should inform participants that "observation" is taking place, and that any information exchanged may be used for research purposes when observing a chat room that is not open to the public.

1.5 Online consent may not be suitable for high risk studies where the research involves data that:

1.5.1 places participants at risk of criminal or civil liability, or

1.5.2 could damage their financial standing, employability, insurability, reputation, or

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, e-mail solicitation, banner ads) must follow the IRB guidelines for recruitment that apply to any traditional media, such as newspapers and bulletin boards.

2.3 Investigators requesting to recruit through USA's mass email system must follow 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 research (45 CFR 46.111), for informed consent, and voluntary participation as all other research activities under the jurisdiction of the USA IRB.

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 subjects should be eliminated from research data or completely encrypted. Researchers might find it most practical to assign research subjects random or generated serial numbers; a map or table correlating these research IDs to personally identifying data could be maintained in a separate file or table which is stored more securely and only accessed as needed.

5.4 It is recommended that data backups be stored in a safe location; this could simply be locked storage in a departmental office, but a secure data room that is environmentally controlled and has limited access is desirable.

5.5 It is recommended that either the researcher or the computer system administrator destroy unneeded copies or backups to ensure that no data can be recovered from obsolete electronic media. If the data are stored on a server system, the researcher should determine not only what procedures are followed to back-up the data, but what provisions are in place to protect the backup media against inappropriate access and how long backups are maintained. Special provisions may need to be made so that confidential research data do not reside on backup media unknown to the researcher.

5.6 The IRB must approve the method and procedures for data collection and security. NOTE: When posting a survey online via a third party (e.g., Survey Monkey, Zoomerang, etc.), the company's security plan for data access and storage must be submitted to the IRB for review and approval.

6.0 Server Administration

A comprehensive definition of appropriate procedures for server management is outside the scope of this document. However, they would include monitoring of vendor and third-party alerting services for security and other updates and application of them as required, logging and monitoring client accesses, establishing and monitoring appropriate file permissions and logon access controls, as well as periodic audits of all security mechanisms. If a departmental server or other network-accessible system is to be used, the researcher should submit to the IRB a description of the security policies and procedures in place. The system administrator of the server in question should be able to provide this information.

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 re-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