Internet-Based Research

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 in the social and behavioral sciences, they present new challenges to the protection of research participants. UNA's HSC believes that computer- and internet-based research protocols must address fundamentally the same risks (e.g., violation of privacy, legal risks, and psychosocial stress) and provide the same level of protection as any other types of research involving human participants. All studies, including those using computer and internet technologies, must (a) ensure that the procedures fulfill the principles of voluntary participation and informed consent, (b) maintain the confidentiality of information obtained from or about human participants, and (c) adequately address possible risks to participants including psychosocial stress and related risks.

At the same time, the HSC recognizes that computer- and internet-based research presents unique problems and issues involving the protection of human participants. The HSC also recognizes that computer and internet technologies are evolving rapidly, that these advances may pose new challenges to the protection of human participants in research, and that both the HSC and researchers employing new technologies must maintain their diligence in addressing new problems, issues, and risks as they arise in the coming years.

Although a formal policy for computer and internet-based research has yet to be ratified, the HSC recommends that researchers adhere to the following procedures to ensure the adequate protection of their research participants and guarantee the validity of the data collected. The purpose of the procedures outlined below is to help researchers plan, propose, and implement computer- and internet-based research protocols that provide the same level of protection of human participants as more traditional research methodologies. This guidance is consistent with the basic HSC principles applied to all research involving human participants.

Recruitment

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

2. Investigators are advised that unsolicited email messages to multiple users are prohibited unless explicitly approved by the appropriate UNA authority. All messages must show accurately from where and from whom the message originated, except in the rare, specific cases where anonymous messages are invited.

3. Investigators are advised that authentication—that is, proper qualification and/or identification of respondents—is a major challenge in computer- and internet-based research and one that threatens the integrity of research samples and the validity of research results. Researchers are advised to take steps to authenticate respondents. For example, investigators can provide each study participant (in person or by U.S. Postal Service mail) with a Personal Identification Number (PIN) to be used for authentication in subsequent computer- and internet- based data collection.

See also UNA policy on Recruitment Material.

Data Collection

1. It is strongly recommended that any data collected from participants over computer networks be transmitted in encrypted format. This helps insure that any data intercepted during transmission cannot be decoded and that individual responses cannot be traced back to an individual respondent.

2. It is recommended that the highest level of data encryption be used, within the limits of availability and feasibility. This may require that the participants be encouraged or required to use a specific type or version of browser software.

3. Researchers are cautioned that encryption standards vary from country to country and that there are legal restrictions regarding the export of certain encryption software outside US boundaries. See UNA's Export Control Policy at http://www.una.edu/sponsored-programs/guidelines-for-grants-and-contraccts.html.

Server Administration

1. It is recommended that for online data collection a professionally administered server be used.

2. If researchers choose to run a separate server for data collection and/or storage, the HSC recommends that:

a. The server is administered by a professionally trained person with expertise in computer and internet security (see d and e below).
b. For security reasons, the server address (URL) is a una.edu domain name.
c. Access to the server is limited to key project personnel.
d. There are frequent, regularly scheduled security audits of the server.
e. The server is subject to the periodic security scans of servers within the UNA domain.

Data Storage/Disposal

1. If a server is used for data storage, personal identifying information should be kept separate from the data, and data should be stored in encrypted format.

2. 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.

3. It is recommended that competent data destruction services be used to ensure that no data can be recovered from obsolete electronic media.