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 of human participants as more traditional research methods. The purpose of the procedures outlined below is to help researchers develop computer- and internet-based research protocols that provide adequate protection of human participants in research and the basic HSC principles applied to all research involving human participants.

Recruitment

1. Computer- and internet-based procedures for advertising and recruiting participants (e.g., internet advertising, email solicitation, etc.) must follow the same guidelines for recruitment that apply to any traditional recruitment method, such as posting on bulletin boards.

2. Investigators are advised that unsolicited email may not be sent to potential participants unless explicitly approved by the appropriate UNA authority. Investigators should use a Personal Identification Number (PIN) to be used for authentication in subsequent phases of 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 scan 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.