Guidelines for Computer- and Internet-Based Research Involving Human Participants

Computer- and internet-based methods of collecting, storing, utilizing, and transmitting data in research involving human participants are developing at a rapid rate and present new challenges to the protection of research participants. The Institutional Review Board (IRB) believes that computer- and internet-based research protocols must address fundamentally the same risks (e.g., violation of privacy, legal risks, psychosocial stress) and provide the same level of protection as any other types of research involving human participants. Both the IRB and researchers employing new technologies must maintain their diligence in addressing new problems, issues, and risks as they arise in the coming years.

The following guidelines are comprised of requirements and recommendations that are consistent with the basic IRB principles applied to all 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.

RECRUITMENT:

1. 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 and must be approved by the IRB prior to posting.
2. Recruitment in chat rooms or on discussion boards must be guided by the level of privacy expected by participants. Sites that require user login or invitation are not considered "public" and the researcher must get permission from the site administrator and fully disclose their intent to the administrator.
3. Investigators are advised that University policies prohibit unsolicited group e-mailings to faculty, staff, and students. Permission to include university employees or students must be obtained by the appropriate supervisor of the group to be included in the research. If the supervisor is unable to give access to a university email list, then the researcher must contact ITS for email addresses once supervisor and IRB approval has been given.
4. 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.

DATA COLLECTION:

1. It is strongly recommended that any data collected from human 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 study 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.

SURVEY ADMINISTRATION:

1. It is recommended that for online data collection a professionally administered survey server be used. The IRB recommends UWG researchers use Qualtrics for which the university has a license for faculty, staff, and student research use.
2. If researchers choose to a survey administrator other than Qualtrics for data collection and/or storage, the following information must be provided in the IRB application materials:
   a. A statement of the security, privacy, and confidentiality practices of the survey provider;
   b. A statement regarding specifically who at the provider may have access to the collected data;
   c. A statement regarding the frequency of security audits of the server where data is stored;
   d. A statement from the survey provider as to who owns the data collected; and
   e. Certification from the survey provider that research data can be deleted/removed from the site and cannot be recovered.

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.

CLOUD COMPUTING:

1. The UWG IRB advises against the use of cloud computing in the research setting. Examples include the following types of third party services: Social Networking Services, Online Backup Services (e.g., Dropbox), Google Docs, Network Storage, Web-based Email (e.g. Gmail, Hotmail, including UWG email addresses).
2. Identifiable research information cannot be stored on a third party cloud computing environment unless specifically approved of by the IRB.
3. Information stored in a cloud computing environment may be considered the cloud vendor's data. If you opt to use these services for storing anonymous data, be aware of the vendor's usage policy and privacy policy.

INFORMED CONSENT PROCESS FOR INTERNET-BASED RESEARCH:

1. For anonymous Internet-based surveys, it is sometimes appropriate to use implied informed consent. Participants would still need to be presented with the consent information, but would be informed that their consent is implied by submitting the completed survey.
2. Other Internet-based surveys include "I agree" or "I do not agree" buttons on the website for participants to click their choice of whether or not they consent to participate.
3. Instead of "signed" informed consent, the researcher may email the consent form to participants who may then type their name and the date into the spaces provided on the consent form, and return it to the researcher via email, if the IRB determines that some sort of documented consent is required.
4. Researchers conducting web-based research should be careful not to make guarantees of confidentiality or anonymity, as the security of online transmissions is in question. A statement in the informed consent form indicating the limits to confidentiality is typically required. The following statement may be used: "Confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties."

Additional information from the U.S. Department of Health & Human Services: Attachment B: Considerations and Recommendations concerning Internet Research and Human Subjects Research Regulations, with Revisions (March 2013).