GUIDELINE FOR COMPUTER AND INTERNET BASED RESEARCH

The purpose of this guideline is to help researchers plan, propose, and implement computer and internet-based research protocols that provide the same level of protection of human subjects as more traditional research methodologies.

Computer and internet-based research protocols that include various methods of collecting, storing, utilizing, and transmitting data 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 subjects. The RSRB will review such non-exempt research protocols using the same considerations and standards of approval of research (45 CFR 46.111) as all other research activities. 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 subject's privacy, (c) maintain confidentiality of information obtained from or about human subjects, and (d) adequately address possible risks to subjects including psychosocial stress and related risks.

Internet-based research may not be suitable for greater than minimal risk studies where the research involves data that:

1. places subjects at risk of criminal or civil liability; or
2. could damage their financial standing, employability, insurability, reputation; or
3. could be stigmatizing; or
4. could result in stolen identity.

Recruitment

1. What requires RSRB review and approval?

   Computer and internet-based procedures for advertising and recruiting potential study subjects (e.g., internet advertising, e-mail solicitation, banner ads) must follow the RSRB requirements for review and approval that apply to any traditional media related recruitment materials (e.g., newspapers and bulletin boards).

2. What does a researcher need to consider to ensure the validity and reliability of data?

   The proper qualification and/or identification of respondents (authentication) may impact the integrity of research data and the validity of research results. Therefore, researchers are advised to consider steps to authenticate subjects in order to minimize misrepresentation of self in internet-based research. Strategies to do so may be implemented with the use of technical software, analytical strategies, or at the time of recruitment/enrollment[1]. Examples below are dependent on the purpose of the study, type of data collected, and available resources, so it is important to consider the proportion of potentially invalid respondents that would be acceptable to complete the study in order to determine which strategies may best be applicable to the study.

   - Technical Strategies – to avoid respondents completing the study multiple times.
     - Assign unique user names and passwords to each subject.
     - Provide each study subject (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. The PIN used must not be one that could be used by others to identify the individual (e.g. social security number).
    - Track the computer IP address of individual respondents (if not using a central computer supplied by the research team); although there are limitations when individuals access the Internet at public locations.
    - Only allow enrollment/participation from approved web links (URLs).

- Analytical Strategies – to identify highly unlikely or unexpected response patterns.
    - Identify pairs of items that can be examined together to evaluate the logic of an individual participant's responses.
    - Analyze whether responses deviate from previous similar research.
    - Collect information that valid respondents should have memorized such as email, addresses, phone numbers or names at various points during data collection and exam to verify consistency throughout the study. This may not be appropriate based on the nature and sensitivity of the study (i.e., anonymous survey) or the target population (e.g., individuals with cognitive impairments).

- Recruitment and Enrollment Strategies – to minimize the ability of a subject to misrepresent him/herself.
    - Limit automatic and open access to web-based data collection.
    - Require potential subjects to complete eligibility questions that demonstrate knowledge of information not familiar to the general population, such as terms unique to a specific population or culture. For research that is not anonymous, the responses may be monitored prior to enrollment, or may be analyzed for discrepancies in the information as compared to that reported during data collection.
    - Based on the research activity and level of risk, it may be appropriate to screen out minors by checking for internet monitoring software such as SafeSurf® and RSACi rating system or other content rating system. Alternatively, age may be verified by asking the subject to enter date of birth as well as age.

Informed Consent Process

For internet-based surveys, it is usually appropriate to use implied informed consent. Subjects would still need to be presented with the consent information, but would be informed that their consent is implied by submitting the completed survey (see RSRB website for applicable consent form templates).

1. When using a consent form, information sheet, or introductory text on the internet site, ensure there is a statement reminding subjects to only complete the requested information one time.

2. For anonymous internet-based surveys, include "I agree" or "I do not agree" buttons on the website for subjects to click to indicate their active choice of whether or not they consent to participate. For anonymous surveys sent to and returned by subjects through email, include an information sheet with consent information and inform subjects that submitting the completed survey implies their consent.

3. If the RSRB determines that written consent is required, the consent form can be mailed or emailed to the subject who can then sign the form and return it via fax or postal mail. Should email or facsimile communications be used, if applicable, refer to the University of Rochester HIPAA Policy 0P29 to ensure subject privacy is adequately maintained.

4. Researchers conducting web-based research should be careful not to make guarantees of confidentiality or anonymity, as the security of online transmissions is not guaranteed. A statement in the informed consent form or information sheet indicating the limits to confidentiality is suggested, such as the following, "Your 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."

5. For research involving minors, Policy 601 Research Involving Children should be referenced to determine whether parental permission and/or child assent may be required.

NOTE: For sections that follow regarding the use of information systems
Researchers under URMC and Affiliates covered entity should refer to the HIPAA Information Security Procedure 0SEC07 Asset Management for additional guidance on using and maintaining secure systems. In addition, the University of Rochester Information Technology Policy or the URMC Information Systems policy and procedures should be referenced as applicable.

Data Collection

1. It is strongly recommended that any data collected from human subjects over computer networks be transmitted in encrypted format. This helps ensure the confidentiality of the data such that any data intercepted during transmission cannot be decoded and that individual responses cannot be traced back to an individual respondent.

2. The level of security should be appropriate to the risk. For most research, standard security measures like encryption and secure socket layer (SSL) will suffice. However, with sensitive topics additional protections may include certified digital signatures for informed consent, encryption of data transmission, and technical separation of identifiers.
    - 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.

3. Internet-based survey instruments must be formatted in a way that will allow subjects to skip questions if they wish, or provide a response such as “I choose not to answer.” Also, at the end of the survey, there should be two buttons: one to allow subjects to discard the data and the other to submit it for inclusion in the study. Finally, if applicable, online surveys must include mechanisms for withdrawal. For example, if a subject decides to withdraw, there should be a mechanism for identifying the responses of a subject for the purposes of discarding those responses.

4. Websites must comply with the applicable University information system policies (links referenced above).

5. Investigators conducting research online with children under 13 are subject to the Children’s Online Privacy Protection Act (COPPA – http://www.coppa.org) in addition to human subjects regulations. Researchers 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 by mail or fax, or potentially by phone. If the research is more than minimal risk, parental permission should be obtained in a face-to-face meeting. Policy 601 Research Involving Children should also be referenced for additional information regarding regulatory requirements and UR policies for research that involves children younger than 18 years of age.

Server Administration

1. Use of SurveyMonkey.com, Psychsurveys.com and other online survey tools is permitted for minimal risk studies that do not involve the collection of sensitive data. As noted above, the RSRB recommends that data be transmitted in a secure format. Therefore, researchers who wish to use SurveyMonkey should upgrade to a Professional account which offers SSL encryption. Psychsurveys offers SSL encryption for all studies. The level of encryption used by the online survey tool must be described in the study protocol.

2. For more than minimal risk studies that involve the collection of sensitive data, the RSRB recommends it be housed on a UR server. The server should be administered by a professionally trained person with expertise in computer and internet security. Access to the server should be limited to key project personnel. The server should receive frequent, regularly scheduled security audits.

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.

Privacy, Anonymity and Confidentiality

There are additional considerations that need to be addressed for maintaining anonymity, privacy, and confidentiality of subject's and their data when developing a research study that will be conducted using computer or internet services, particularly when considering the nature and sensitivity of the study.

- *Anonymity:* Information gathered from internet based research usually maintains anonymity; however, consider whether IP address will be collected, and if so, whether that may lead to a potential for matching to a specific individual (e.g., use of a centralized computer supplied by the research team versus IP address from an individual's personal computer). Use of email accounts may be more prone to lack of anonymity; however, the risk is reduced if, for example, data received is immediately transferred to a data file coded by generic subject number rather than email address.

- *Confidentiality:* There is the potential for confidentiality of data to be compromised during data transmission and storage, so it is important to consider methods that will be implemented, as applicable, to mitigate that risk. When using email communication, understand the potential implications that may arise, such as more than one person having access to an email account, the email being re-routed to unanticipated locations due to technical malfunctions with the computer network, the email being sent to the wrong address, ensuring people understand to reply privately to a message rather than replying to an entire listserv or other group.

[1]Kramer et. al. Strategies to Help Ensure Validity of Web-based Research Samples. Clinical Research Times Boston University Medical Center. February 2012 Issue.