



---

**SUBJECT: Guidance on Conducting Computer – and Internet-Based Research  
Involving Human Subjects**

Internet data collection via email, list serves, 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 computer and internet based research activities, including subject recruitment, in human subjects research to ensure that:

- (1) Risks such as violation of privacy, legal risks, psychosocial stress are minimized;
- (2) Subjects' participation is voluntary;
- (3) Informed consent requirements are met; and
- (4) 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.

Electronic mail poses additional risks in the handling of confidential data. Data may quite readily be transmitted to unintended recipients through misaddressing or similar error. In addition, the routine maintenance of mail systems may require or inadvertently lead to viewing of some pieces of mail by mail systems administrators. In general, email should be avoided for the transmittal of confidential data, unless encrypted.

The IRB recommends that researchers follow the procedures outlined below to ensure the adequate protection of research participants and guarantee the validity of the data collected. This guidance will assist researchers plan, propose and implement computer – and internet-based research studies while providing the same level of protection of human subjects involved in more traditional research studies.

The following guidelines are as follows:

**A. IRB Application/Recruitment:**

1. The procedures for using USA's mass email system are documented at <http://www.southalabama.edu/emailprocedures.html> . All messages must clearly indicate from where and from whom the message oriented. This recruitment procedure must be approved in advance by the IRB.
2. Section entitled "Recruitment/Compensation": State the procedures to be employed to authenticate that the participants are adults. Additionally, state plans to use a secure server. Stripping identifiers from data, storing identifiers and data in separate files and auditing the security of data directories should be routine procedures.
3. Section entitled "Consent Process": Request an IRB waiver of signed consent if subjects do not involve participation of minors. The IRB has the authority to waive this requirement if the study meets requirements as outlined in 45 CFR 46, Section 117 (<http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm>)

**B. Consent Document:**

1. Informed consent should be obtained prior to responding to survey instruments by having the first page as an information sheet and consent form rather than the actual survey.
2. An Internet consent document should be written like a cover letter and should include all the elements of the regular signed consent, including the confidentiality disclaimer given below. The consent line should say, "By completing the survey you are agreeing to participate in the research". Internet-based surveys should 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 study participation.
3. Investigators conducting Internet-based research should be careful not to make guarantees of confidentiality or anonymity, as the security of online transmissions cannot be ensured. Therefore, the following confidentiality disclaimer should be included in the consent document, "There is a limit to the confidentiality that can be guaranteed due to the technology itself."
4. Once participants have read and acknowledged the consent information, they should be able to print a copy.

5. Online consent is not suitable for high risk studies where research involves data that:
  - o Places subjects at risk of criminal or civil liability, or
  - o Could damage their financial standing, employability, insurability, reputation, or
  - o Could be stigmatizing.

**C. Survey Instrument:**

1. The instrument should be formatted in a way that will allow participants to skip questions if they wish to or provide a response like "I choose not to answer".
2. At the end of the survey, there should be two buttons: one to allow participants to discard the data and the other to submit it for inclusion in the study.
3. Provide an alternative means of filling out the survey. For example, allow the participant to complete it and send it via snail mail to the researcher. Ensure that the researcher's contact information is prominently displayed on both the cover letter and the survey instrument to avoid having the survey misdirected to the IRB.

**D. Data Collection/Storage:**

1. Data collected from human subjects over computer networks should be transmitted in encrypted format. (see Section G "Encryption Guidelines" below)
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)
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.
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. 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 backup 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 .
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.

**E. 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.

**F. Portable Computers and Media:**

Because of the possibility of theft and discovery of data, portable computers (notebooks, laptops, etc.) and portable storage devices, including USB keys and portable disks, should **NOT** be used to store confidential research data, unless such data is encrypted.

**G. Encryption Guidelines:**

See The University of Minnesota's Office of Information Technology website at: [http://www1.umn.edu/oit/security/Encrypting\\_Stored\\_Data.html](http://www1.umn.edu/oit/security/Encrypting_Stored_Data.html) The IRB is in the process of developing a local document describing encryption options. For the time being, we refer you to the above referenced website.

**H. Background Information:**

Kraut, R. et al 2004 Psychological Research Online: Report of Board of Scientific Affairs Advisory Group on the Conduct of Research on the Internet. American Psychologist February/March 2004.

Association for the Advancement of Science, Ethical and Legal Aspects of Human Subjects Research on the Internet (.pdf)

American Psychological Association, Psychological Research Online: Report of Board of Scientific Affairs' Advisory Group on the Conduct of Research on the Internet

*This document was prepared in consultation with the Computer Services Center  
June, 2007*