

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

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. Columbia's Morningside 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, 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 IRB recognizes that computer- and internet-based research presents unique problems and issues involving the protection of human participants. The IRB 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 IRB 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 IRB 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 outline 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 IRB 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, e-mail solicitation, banner ads) must follow the IRB guidelines for recruitment that apply to any traditional media, such as newspapers and bulletin boards (see the IRB "[Guidelines for Subject Recruitment and Advertising](#)").
2. Investigators are advised that unsolicited e-mail messages to multiple users are prohibited unless explicitly approved by the appropriate University authority. (See [Mass-Email Procedures](#).) 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.

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.

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 IRB 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 cu.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 Academic Information System (AcIS) security scan of servers within the CU 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.

RESOURCES:

Columbia University Computer and Network Use Policy:

<http://www.columbia.edu/acis/policy/>

Procedures for Sending a Broadcast Email Message at Columbia University:

<http://www.columbia.edu/acis/policy/mass-email-procedure.html>

Ethical and Legal Aspects of Human Subjects Research in Cyberspace; a report from the AAAS Program on Scientific Freedom, Responsibility and Law, in collaboration with NIH/OPRR:

<http://www.aaas.org/spp/sfrr/projects/intres/report.pdf>

Procedures for Sending a Broadcast Email Message at Columbia University

Version 1.14, December, 2001

1. Any request to send a broadcast email message to students, faculty and/or staff in more than one school or administrative unit must be approved by the Deans or Senior Administrators of all the affected units; or the President, Provost, or Executive Vice President for Administration; or authorized by a resolution of the University Senate.

Where the members of affiliated institutions are to be included, the President, Provost, or other authorized official of each institution must approve the inclusion of its members in the mailing.

2. The timing of the message must be approved by the Deputy Vice President for Academic Information Systems or his representative. Call 854-1919 for assistance.

The mailing must also be coordinated with the University's e-mail postmaster (postmaster@columbia.edu) to ensure that it will not disrupt the email system. Normally, delivery will be scheduled to begin after 9:00 PM.

The sender may also request, from the postmaster, a special shared email file for any responses to the mailing.

3. a. For mailings to **Columbia students**.

Setting up the list of recipients, allowing the sender to send to the list, and coordinating delivery is handled by Student Information Systems (SIS), call 854-2989 or mail infoline@columbia.edu.

- b. For mailings to **Columbia faculty or staff**.

Setting up the list of recipients, allowing the sender to send to the list, and coordinating delivery is handled by Human Resources, call Sue Spencer at 870-3106 or send e-mail to ses24@columbia.edu.

- c. For **combined mailings to Columbia students, faculty, and/or staff**.

Coordinating setup, list access, and delivery is handled by the Assistant Director, Academic Information Systems. Call 854-7455 or 854-1919.

d. For mailings including **members of other institutions**.

Access to lists and sending messages must be arranged with the appropriate technology offices.

4. The sender of the message will be given authorization to use the list only for the approved message.
5. The headers of the message or the mailing list must include a Reply-to: with an individual, group, or file address where replies will be received and responded to as appropriate. This need not be the sender. As noted above, reply mailboxes can be requested from `postmaster@columbia.edu`.

Note that the mailing lists are set up so that individual recipients cannot reply to the lists or send messages to them.

The Reply-to: address should also be mentioned in the text of the message and a telephone number and office address for other inquiries should also be given.

The initial text of the message should indicate that it is a broadcast and which office is sending the message:

"This is a broadcast message from ..."

6. The inclusion of attachments in broadcast messages is not allowed because of the possibility of spreading a virus and possible incompatibility with the recipient's system.
7. Except in emergencies, five working days notice is required for any such mailing. In any case, several hours may be required to set up such a mailing, and the message is sent in batches over another several hours so as not to compromise normal email delivery.