

Appendix B Requirements for Online Surveys

As methods of computer- and internet-based research with human participants become more widely used, they present expanded opportunities for conducting surveys while also creating new challenges in complying with requirements for the protection of research participants. The CPHS believes that computer- and internet-based research protocols must address the same risks (e.g., psychological stress, feelings of guilt or embarrassment, invasion of privacy, inadequate protection of confidentiality) and provide the same level of protection as the more traditional non-electronic methods of research involving human participants. All studies, including those using computer and internet technologies, must:

- ensure that the procedures meet the principles of voluntary participation and informed consent
- maintain confidentiality of the information obtained from or about human participants
- adequately address the possible risks to participants, including psychological, social, and economic risks

The purpose of these guidelines is to help researchers develop computer- and internet-based research protocols that provide protection for human participants comparable to more traditional research methodologies, and to explain the additional information that researchers must provide when they submit applications that involve online surveys to the CPHS.

Recruitment

As with any other research study, the recruitment materials for online research and the context in which the recruitment takes place (including electronic methods such as posting a message on a newsgroup or creating a website to recruit participants) must be reviewed and approved by the CPHS.

Investigators should be aware that authentication (establishing the qualifications 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. If the respondent population is not the population that was originally targeted by the researcher, the resulting data may not reflect what the researcher intended to assess. Investigators are advised to take steps to authenticate their respondents. For example, investigators can provide each participant (in person or by U.S. mail) with a Personal Identification Number (PIN) to be used for authentication in subsequent computer- and internet-based data collection.

Online Data Collection and Storage

The CPHS requires that any data collected from human participants over computer networks

be transmitted in an encrypted format. This helps to ensure that any data intercepted during transmission cannot be decoded and that individual responses cannot be traced back to an individual respondent. The highest level of data encryption should be used, within the limits of availability and feasibility. 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 U.S. borders.

If a server is used for data storage, any personal identifying information should be kept separate from the data, and the data should be stored in an encrypted format.

Informed Consent

1. Internet consent documents should be written like a cover letter and should include all of the elements of a regular signed consent, including the confidentiality disclaimer given below. The consent line should say, "By completing this survey, you are agreeing to participate in the research". Internet-based surveys should include "I agree" and "I do not agree" buttons on the website for participants to click their choice of whether or not they consent to participate.
2. The following statement must be included in the consent form: "Your responses will be kept confidential to the degree permitted by the technology used. However, no absolute guarantees can be given for the confidentiality of electronic data."
3. The consent form must disclose that if a participant completes an anonymous survey and submits it, the researcher will be unable to remove anonymous data from the database should the participant wish to withdraw it.
4. Depending on the level of risk in the research, the CPHS may not be able to waive the usual requirement for obtaining a signed written consent from participants. In that case, the researcher will need to distribute a printed consent form and acquire a signature before the participant is given information about how to access the online survey.

Survey Software Checklist

The following checklist specifies the protections which the CPHS expects any online survey software to have. The answer for each question should be "Yes". An answer of "No" to any of questions 1-4 or 6 would disqualify the survey software from being approved. Researchers should contact their survey software company to determine whether the software meets these criteria. The application submitted to the CPHS must include the researcher's answers for these questions and the supporting evidence from the company.

1. Informed consent

- Does the software provide the researcher with a record that captures the participant's consent before starting the survey?
- Is that record logged with a time and date stamp (e.g., "respondent #12 consented at 21:27:13 on 05-Jun-2008")?

2. Secure transmission

Information can be sent to and from websites either in clear text (*http* protocol) that could be read if intercepted by a third party, or in encrypted format (*https* protocol) that could not be read by a third party intercepting the information.

- Does the survey software use *https* encryption?
- Does the software prevent a respondent from accidentally entering survey data via the *http* protocol instead of the *https* protocol (i.e., does the server display an error message or automatically re-route the respondent to an *https* page)?

3. Database security

- Is access to the research database limited to authorized persons by means of a username and password?
- Has the software company that maintains the research database signed a confidentiality agreement that prevents it from improperly accessing or disclosing the information contained in research databases?

4. Server security

- Are the servers that contain the research data located in a data center that has physical security and environmental controls?

5. Backups

- Is the data backed up nightly?
- Is there a limited time period in which a deleted dataset can still be retrieved but after which the data will be permanently destroyed? (The investigator should inquire how long this time period is.)

6. IP addresses

- Is the respondent's IP address masked from the researcher?