Internet Research: human research protection in cyberspace

Is an avatar a human subject?
Is a chat room a public forum?
Can information available via the Internet ever be considered as “private”?
How do researchers obtain informed consent or parental permission from participants of Internet Research?
How does legal jurisdiction apply in Internet research?

Questions such as these have confounded researchers and IRB’s alike. In March, a subcommittee of the Secretary’s Advisory Committee on Human Research Protections (SACHRP) presented a working document entitled, Considerations and Recommendations Concerning Internet Research & Human Subjects Research Regulations. The document is described a starting point for the development of FAQs and points to consider regarding the conduct and review of Internet research. It is important to note that the recommendations are preliminary and have not yet been adopted by any federal agency. However, the content may be helpful as researchers and IRBs work through the issues.

Internet research covers a broad range of activities from using the Internet as a tool, such as in recruitment, to using it as a venue for research, as seen with web-based surveys. Applying concrete regulations to online activities in cyberspace is not a simple task. The absence of face-to-face contact elicits both human subject protection and data integrity concerns. Practical strategies are needed to help researchers screen out minors, prevent duplicate entries, authenticate subject identity, ensure adequate informed consent, minimize risk of a breach of confidentiality, etc?

Determining when Internet activities meet the regulatory definition of human research requiring IRB review, requires interpretation of what information is considered public vs. what is disclosed with an expectation of privacy. Colorado State University has defined criteria to aid their researchers and IRB in determining when research in social networks [pdf], public sites [pdf], and virtual worlds [pdf] meets the definition of human subject research requiring IRB review.

A central issue for Internet research is data security to protect participant identity and secure private information. Typically the greatest vulnerability for a breach is during the time the web based program is open and being used by the participant. The UK Confidentiality and Data Security Guidelines for Electronic Data provides recommendations for data security including resources for web-based surveys. The UK Information Technology Security Office also provides technical tips, support, and security awareness materials for posting or distribution.
Changes to the Continuation Review Report Form

A new item has been added to the Continuation Review (CR)/Final Review report form which asks the Principal Investigator (PI) to submit a brief summary of any modifications approved by the IRB since initial review or the last continuation review, which may impact subject safety or welfare. Both Office of Human Research Protection (OHRP) and Food and Drug Administration (FDA) guidance documents indicate that Continuation Review progress reports should include “a brief summary of any amendments to the research approved by the IRB since the IRB’s initial review or the last continuing review.”

The Office of Research Integrity is revising Modification Approval letters to help remind investigators of this requirement at continuation review time.

Another new item on the CR report form replaces a question asking where the records containing signed consent/assent documents are located. The new item references the Confidentiality section of the Research Description (“Form B”), and prompts for an update if there is not already a description of the measures established for security of electronic and physical research records (e.g., informed consent documents, HIPAA Authorization forms, sensitive or private data).

For tips on preparing a Continuation Review submission, see the March 2013 IRB Review Newsletter.