2007

HRPO internet research guideline

Sarah Fowler-Dixon
Washington University School of Medicine in St. Louis

HRPO Internet Research Guideline

Presented by:

Sarah Fowler-Dixon, PhD

Nov. 2007 Brown Bag

NOTE

- This guideline is posted on the HRPO website at: http://hrpohome.wustl.edu/study_team/guidelines.aspx under General Guidelines

DEFINITION OF INTERNET RESEARCH

- Any activity meeting the definition of “human subject research” which is designed to recruit participants or collect data via the Internet

Examples

- questionnaires completed online via the Internet regardless of access code (examples of access codes include UserIDs, passwords, security pictures, etc.)
- questionnaire downloaded from a server on the Internet and returned by mail
- questionnaire incorporated into an e-mail and returned the same way
- qualitative interviews or discussions conducted over the Internet
- taking part in a measurement system which tracks web usage using specialist software installed on the user’s computer
- experiments conducted over the Internet

Examples

- use or housing of large public use databases
- recruiting volunteers over the Internet
- observation of individual behaviors via the Internet (e.g., “chat rooms”)

CONSIDERATIONS when conducting research

over the Internet

Vulnerability

- Discuss how vulnerable the community is (e.g. a mailing list for victims of sexual abuse or a chat room for parents talking about child rearing theories).

Potential harm

- Does the intrusion of the researcher or publication of results have the potential to harm individuals or the community as a whole.

Intellectual property rights

- In some cases, participants may seek publicity so the use of postings without attribution may not be appropriate.

Age of the participant

- On the Internet age is difficult to verify.

- To exclude minors, the researcher may state the minimum age of participants on a webpage at the outset of the study and state that the individual should press the "not eligible, please discontinue" button (give the location) if they are not yet 18 years old. An alternative method that has been employed is to ask the participant to provide his/her date of birth. There are programs that perform the calculations and proceed accordingly.

CONSENT ISSUES

- What type of consent is needed (waiver of consent, waiver of written consent, full written consent, use of cover sheet that incorporates all 8 elements of consent)?
- What is the wording of the consent?
- How will consent be acknowledged?
- Will this be traceable or identifiable? Can the participant be retraced using the IP address?
- Will protected health information (PHI) be transmitted? If "yes," special considerations apply. Further guidance can be found on the Washington University HIPAA website at http://hipaa.wustl.edu or by calling the HRPO office at 314-633-7400.

CONSENT ISSUES

certain information must be conveyed to the participants:

- that the Internet has an inherent unsecured nature.
  - “https” or that display a small padlock are considered secure.
- may be accessed by employers, or using computers or e-mails shared with others.
  - Shared computers may also contain tracking devices that allow others to “see” what sites have been accessed or what key strokes were used.
- that the participants should completely log off the computer when finished with the session for the day to help maintain privacy.

CONSENT ISSUES

certain information must be conveyed to the participants:

- Internet temporary files and cookies should be deleted so that subsequent users can not “see” what sites others have visited.

- The participant must agree, by clicking a button (marked yes, accept, agree, etc) or by continuing, to accept the risks of Internet research and accept the confidentiality and privacy limitations.

PRIVACY

- What is the perceived level of privacy for that community?
- Is it a closed group requiring registration?
- What is the membership size?
- What are the group norms?
- What information is being collected about the participants (e.g. name, address, social security number, phone number, etc). How will this be protected? How long will this information be kept in an identifiable format?

Confidentiality

- How can the anonymity of participants be protected (if verbatim quotes are given, originators can be identified easily using search engines, thus informed consent is always required)?
- Is the information being sent via secure sites using encryption?
- Will participants be re-contacted? If “yes,” the information is not de-identified.

Intrusiveness and Private vs. Public space

- To what degree is the research being conducted intrusive (passive analysis of Internet postings versus active involvement in the community by participating in communications).

- HRPO must consider whether participants' right to privacy is being jeopardized when research is conducted in a covert manner. Under most circumstances, HRPO will require that investigators inform participants that they are being observed for research purposes. This may involve requiring the investigator to contact the web master to obtain permission or other forms of active or implied consent.

Does HIPAA Apply?

- The Internet environment is not considered a covered entity.
- However, placing individually identifiable information in a medical record is considered PHI and HIPAA regulations and policies apply.

Secure Network Standards

- A secure network should be used.
- 1. The entire network is isolated from all other networks by at least one firewall that prohibits all inbound connecting traffic (other than through a VPN) to computers housing electronic PHI.

  2. All devices comprising the physical network -- routers, switches, VPN gateways, firewalls, etc. -- are configured, managed, and monitored by one organization solely responsible for the entire secure network.

Secure Network Standards

- 3. Domain Name Service (DNS) entries for devices housing electronic PHI on the secure network will not be broadcast outside of the secure network.
- 4. Internally, the secure network will utilize network devices that prohibit connected devices (such as network sniffers) from eavesdropping on network traffic. Diagnostic sniffing by authorized network management is allowed.
- 5. All data traffic entering and exiting the secure network via the VPN gateway(s) and firewall(s) must be logged. Logs will be maintained for 12 months.
- 6. All network computer equipment (routers, switches, etc.) should be physically secured and access should be controlled.