

Internet Research & Electronic Data Security

Jeffrey M. Cohen, Ph.D. CIP
President
HRP Associates, Inc.

© HRP Associates, Inc.



Internet Research

IRB Issues

- Research on the Internet presents new concerns to the traditional IRB issues of:
 - Risk/Benefit
 - Consent
 - Participation by minors
 - Confidentiality.

Risk

- Two sources of harm:
 - participation in the research
 - No direct contact with subjects
 - Can't deal with individual reactions (intervention or debriefing)
 - breach of confidentiality
 - Primary source of harm in most internet research

Benefits

- Conducting research on the Internet raises concerns about the reliability and validity of the data.
 - skewed subject populations
 - ease with which subjects can mislead investigators
 - difficulty in preventing multiple submissions
- Invalid research can have no benefit.
 - inappropriate when there is risk to subjects

Consent

- IRBs can waive the requirement for consent where appropriate [45CFR46.116(d)].
- If consent is required, IRBs can waive the requirement for documentation of consent where appropriate [45CFR46.117(c)].

Consent

- Where consent required but documentation is waived, a “portal” can be used to provide consent information.
 - Subjects must click on Consent page to get to next page.
- Where written consent required, it is currently not possible to get a signed consent form over the Internet.
 - Can have subjects submit signed consent form and get password for access to web site.

Participation by Minors

- Where research qualifies for waiver of parental permission, no additional safeguards are required.
 - Either minors can participate without permission or a simple statement in consent that participant is over 18 is sufficient
- Where parental permission required, see previous options for consent.

Participation by Minors

- To screen out minors:
 - use Internet Monitoring software (SafeSurf and RSACi ratings)
 - use Adult Check systems
 - None of these are foolproof.
- Since there is no guarantee that minors won't access research, some research may not be appropriate for the Internet.

Privacy & Confidentiality

- Research on the Internet presents new concerns to the traditional IRB issues of privacy & confidentiality
- Privacy concerns relate to whether Internet activity
 - Is identifiable
 - Constitutes public or private behavior
- Confidentiality concerns relate to inappropriate disclosure of information obtained over the Internet

Privacy

- Identifiable vs. Anonymous
 - Online participants usually use pseudonyms (screen names, handles, etc.)
 - Although not publicly linked to actual names, identities can often be “readily ascertained” (e.g., using search engine)
 - People’s online identity may be as important to them as their actual identity

Privacy

- Public vs. Private Behavior
 - Most online activity is open to the public
 - Federal regulations base the definition of “private information” on the subjects’ “reasonable expectation” of privacy
 - In many situations (e.g., chat rooms), participants expect privacy and don’t expect their activity to be studied
 - Determination of privacy more complicated than it seems

Confidentiality

- Two potential sources of breach of confidentiality
 - inadvertent disclosure
 - Investigator who sent out research database to entire Listserv
 - Investigator who's computer was stolen
 - deliberate attempts to gain access
 - No recorded incidents of hacking research data
- Technology can provide reasonable security but cannot guarantee absolute security

Confidentiality

- Data transmitted via e-mail cannot be anonymous without the use of additional steps. Almost all forms of e-mail contain the sender's e-mail address.
 - use an "anonymizer" - a third party site that strips off the sender's e-mail address
- Web servers automatically store a great deal of personal information about visitors to a web site and that information can be accessed by others.

Confidentiality

- Degree of concern over confidentiality depends on sensitivity of the information
- Since it is impossible to guarantee absolute data security over the Internet, some extremely sensitive research may not be appropriate for the Internet

Resources

- American Psychological Association – Report of the Advisory Group on the Conduct of Research on the Internet
<http://www.apa.org/science/apainternetresearch.pdf>
- AAAS Report on Internet Research
<http://www.aaas.org/spp/dspp/sfrr/projects/intres/main.htm>



Electronic Data Security

Risk Analysis

- Sensitivity of data
- Likelihood of interest
- Degree of security directly related to risk

No Guarantees!

- All operating systems have vulnerabilities
- No technology can guarantee against unauthorized access
- Best protection is “defense in depth”
 - Multiple layers of security

Physical Security

- Restricted physical access to computers
 - If someone can access a computer they can breach security
- Locked rooms
- Use password protected screen savers and turn off computers
- Lock computers
 - Locked to tables and locked cases
- Boot from hard drive only

Limited Service on Computer

- Limit web access
- Limit software
 - Web server
 - ftp
 - Mail server
 - Peer to peer
 - Anonymous file sharing

Computer Configuration

- Latest software versions
- Follow manufacturer security recommendations
- Monitor updates and install security patches promptly
- Load anti-virus software and update regularly

Authentication

- Control access privileges
- Access must be authenticated
- Require “strong” passwords
 - Complex (require combination of numbers, uppercase, and lowercase letters)
 - Long (at least 8 characters)
 - Regular changes (e.g., new password every 30 days)

Data Encryption

- Conversion of data into a form that can't be understood by unauthorized people
- Both authentication (user id and password) and data should be encrypted
- Data sent over the Internet should be encrypted
- Data on local machines should be encrypted
- Only use the latest, strong encryption software

Firewalls

- Software that blocks unauthorized data from passing through the system
- Network systems should be filtered
- Hardware should have firewalls installed
- Data directories can have additional firewalls

System Auditing

- Vulnerability scans
 - Vulnerability testing software
- Event and access logs
 - Monitored regularly

Backups

- Backup data regularly
- Evaluate security of system backups
- Secure hard copy backups

Secure Equipment Disposal

- Regular file deletion doesn't delete data
- Need "secure deletion"
 - Overwrites data with random 1s and 0s
- Removable media (CDs, tapes, disks) should be physically destroyed

Technical Support

- Computers and systems must be continually managed and updated
- Tech support must have necessary expertise in data security and stay up to date

IRB Requirements

- Investigators are going to have to provide technical information on how they will deal these issues.
- IRBs need to have sufficient expertise on the technical aspects of the Internet in order to ask the right questions and evaluate the information provided.
- IRBs that review Internet research without sufficient expertise are not in compliance with the regulations!