How IRBs Review Addictions & HIV Digital Media Research

Opportunities and Challenges

Brenda Curtis, PhD, MSPH

Assistant Professor
Department of Psychiatry—Addictions

July 2017

Ethical Challenges

- **Recruitment**
- **Informed Consent**
- **Privacy and Confidentiality**
- **Justice**
- ***Data Validity***

Ethical Considerations

- **Recruitment**
  - When does research begin? Are we giving marketing companies information about people who click our research ads?
- **Autonomy: eConsent**
  - Tech can help us do this better
- **Risk Benefit Determination**
  - **New or Different risks**? **Magnitude of Risks**?

    Are some of the risks, which historically are considered minimal now greater than minimal?
- **Justice Considerations:**
  - Who doesn't have access? (platform specific?)
- **Data validity:**
  - How are you ensuring validity of data while minimizing privacy/confidentiality?

Questions Your IRB Should/Might Ask

"A prudent question is one-half of wisdom."

— Francis Bacon

Important Questions

- **Where do the interactions, communications, and study take place?**
- **What ethical expectations are established by that venue?**

The greater the perceived privacy of the participant and/or the less privacy afforded by the venue, the greater the need to protect individual privacy, confidentiality, and right to informed consent

Important Questions

- **Who are the participants?**

The greater the vulnerability of the participant, the greater our obligation is to protect the participant.

Important Questions

- **When will the informed consent process start?**

Ideally, protecting participants' rights to privacy, confidentiality, autonomy, and informed consent should start at the beginning of any data collection.

Important Questions

- **How long does the third-party provider preserve the data and where?**

Every effort should be made to (a) not store data by third-party providers and (b) if it is being stored, have the data removed as soon as possible.

Researchers need IP addresses to ensure the integrity of the date being collected.

Important Questions

- **What third-party policies impact the research?**

General counsel may be asked to review the terms and services of the sites and any third-party provider contracts.

The researcher should provide adequate information to participants and the IRB concerning how third parties will protect the data.

Your IRB Review

Electronic Data Security

Data management of human subjects research data includes: data collection, data entry, and database repository oversight (controlling access, tracking use of analytic datasets). When reviewing electronic data collection, there are 4 important areas to examine:

Identifiers 1

- What type of identifying information will be collected?

Technologies 2

- What types of technologies will be used in the research study?

Data 3

- Once data is collected, how will it be transmitted, processed, and stored?

Security 4

- During data collection, how will it be transmitted, processed, and stored?

Identifiers

- Name
- E-mail
- SS#
- Phone numbers
- IP address
- Images (photos/face)
- Device identifiers
- Biometric identifiers
- Accounts info
- Address (home/work)
- GPS/location

Technologies

- **Cellphones, Apps, Wearables, Texting, Web-site, electronic recording, video?**
  - Who developed the platform?
  - How will the platform be accessed?
  - How will the data be stored?
  - How is the data coded?
  - Where is the app hosted?
  - Security features of the platform? (end-to-end?)
  - Will GPS data be collected? (can users turn it off?)
  - Is the communication one- or two-way?

Security

- **During data collection:**
  - Who will have access to the data?
  - Is the app developer collecting “other” data? (meta)
  - How will data access be managed?
  - Who is responsible for maintaining the security of the data?
  - Is the device/site/app password protected?
  - Does only the participant access the device/site/app?
  - Is data collection in a private “location”?

Data

- **Once the data are collected, how will it be transmitted, processed, and stored?**
  - Who owns the server?
  - What is the server operating system?
  - Will cloud file storage be used?
  - Will data live on a workstation? Laptop? Tablet?
  - Where will the data be housed?
  - Where is the site/data hosted?
  - Will data be stored on user devices? (protocol for removal?)
  - What is **YOUR** data security plan? Does it align with your **INSTITUTION**?

Compliance Protocol Design

	Who?	What?	Where?	When?	Why?	How?
Data Type	Entered by subject? Auto-collected by device/ platform?	PHI? Survey? GPS? Interaction or usage of device/ platform?	Under what circumstances or situation will it be entered?	By user action? By device/ platform?	Primary data for the study? Data about the device/ platform itself?	What is the detailed mechanism for collecting this?

Investigators and developers should map out all the data collection, and sharing points along with descriptions of the security measures and how it protects the privacy of the subjects

This will go a very long way in terms of explaining the more complicated workings of your research and the technologies you plan to use

Be Prepared!

- **If you prepare a clear, well written, and thought out IRB protocol application, you will have success.**
  - Refer to the national regs
- Refer to articles that used similar methods
- Refer to other protocols your IRB approved that used similar methods
- When possible, explain that this “new technology” is similar to “old” technologies they are more familiar with