AN EMERGING TECHNOLOGIES, ETHICS, AND RESEARCH DATA CASE STUDY

SECURE STORAGE OF AUDIO RECORDINGS

By: Kim Serpico
with the Emerging Technologies, Ethics, and Research Data Subcommittee of Harvard Catalyst’s Regulatory Foundations, Ethics, and Law Program

OVERVIEW

The Emerging Technologies, Ethics, and Research Data case studies provide education and guidance on how to identify, assess, and review research data security issues. These studies may be used by IRB administrators and investigators to identify key issues, considerations, and decision criteria when reviewing and designing research studies that involve data collection and sharing components.

Case studies follow a standard format that includes: 1) a fact pattern, 2) contractual, regulatory, ethical, and technical issues, 3) stakeholder considerations to identify, assess, and mitigate risks, and 4) resolution and points for discussion.

By identifying common themes, linking them directly to federal regulations and guidance, and outlining options, the case studies can be used in a variety of ways, which include: 1) as an educational tool for training individuals in human subjects research, 2) as a basis for developing reviewer checklists/worksheets, and 3) as a tool in designing research projects.

We encourage you to reproduce and use these materials freely. In doing so, we require that you acknowledge Harvard Catalyst as the publisher and that you give appropriate credit to the individual authors. For additional information, visit http://catalyst.harvard.edu/about/citingsupport.html.

CASE STUDY

Scenario/Fact pattern:

Researchers at a local university plan to conduct interviews with human subjects in the field and audio record those interviews. The interview and responses will contain participant identifiers and sensitive personal information about the participant. That said, the information has been shared by the participant with an expectation of privacy and the understanding that it will not be divulged without their permission.
CONSIDERATIONS

Researcher Considerations:

- How will confidentiality of the data be maintained?
- What kind of device will the audio recordings be made on - an encrypted device, tape recorder, smart phone, etc.? If a smartphone is used, are there any automatic cloud backups, such as iCloud, that occur? If so, where is this data copied to? Is it secure?
- In addition to using a secure recording device, the audio files made by the device will need to be managed securely as well. Do you have the resources to encrypt, password protect, and/or securely manage the identifiable audio files? Have you spoken to your local IT security officer to ensure you have the appropriate data security and confidentiality solutions in place to protect the study data?
- What is your plan for audio transcription? How will the original recording be handled after transcription takes place? If you plan to store the audio files indefinitely, what is the justification?
- If recorded data will be transcribed, how will this be done? Will an outside resource – a research assistant or vendor – be used for transcription services? If so, proper contracts should be in place to protect the confidentiality of the data.
- Will the audio files be transmitted in any way? If so, where, when, and how?
- How will you ensure only authorized members of the study team will have access to the audio files?
- Is the principal risk of the study breach of confidentiality? What would be the potential harm to the participant resulting from a breach?
- If a participant withdraws from the study, how will their data/interview be handled?
- Are you familiar with your IRB’s policies on reportable new information (e.g. breaches, data loss, hacking, theft, etc.) in the event of an unexpected issue with the audio files?
- If something is captured during the discussion that either the participant or researcher doesn’t want stored as part of the permanent research record, the recording should be paused and recorded over.
- The consent form needs to appropriately inform participants about how the audio recordings will be stored, managed, and utilized throughout the life of the study.
- There are many record retention obligations that need to be adhered to throughout the life of the study – to the IRB, sponsor(s), journals/publications, federal regulations, etc.

IRB Considerations:

- Is the data storage and management plan adequate?
- How often are the audio files removed from the recording device to their storage location, and by what method?
- Will the researchers monitor the data collected in a timely enough way in order to ensure the safety of subjects?
- Based on the interview questions, could the study data collected, if disclosed outside of the research, reasonably place the participant at risk of criminal or civil liability or be damaging to their financial standing, employability, insurability, or reputation?
● Has the risk of breach of confidentiality, and the researcher’s plans to minimize that risk, been sufficiently explained in the consent form?
● Does the researcher have a plan to permanently destroy the data in the event a participant decides to withdraw from the study and does not want their interview used? Is the communicated in the consent form?

IT Considerations:

● What resources will the researchers need to fulfill IT recommendations to secure the study data?

RESOLUTION & DISCUSSIONS

Per the federal regulations, the IRB must ensure that there are adequate provisions in place to protect the privacy of subjects and to maintain the confidentiality of data. This includes a strong management plan for all stored data, in both digital and paper formats. The IRB also must ensure that the consent form communicates, clearly and appropriately, how participants’ data will be protected and secured, and their ability to withdraw their data should they choose to do so. It is then the researcher’s responsibility to uphold what is written in the consent form, and report any deviations to the IRB. IT can assist the researcher by educating them on secure data storage and management solutions. Audio files are of particular concern because of the ease in which they can be recorded (e.g. on a smartphone) and then improperly secured. Finally, researchers need to be cognizant of all record retention obligations, and indicate what these are and how they will adhere to them in their research protocol.

RESOURCES

Harvard Catalyst Guidance for Researchers Using Internet Cloud Computing Services and Apps

REFERENCES

45 CFR 46 - §46.111 Criteria for IRB approval of research: