EXAMPLE Data Management and Sharing Plan for High Risk Human Subjects Research

Acknowledgement: This document was created by the Research Data Service at the University of Illinois at Urbana-Champaign (UIUC) to provide an example Data Management and Sharing Plan (**"**Plan") for an NIH proposal. We based this Plan off an award-winning DMP for an NSF-SBE application "Religion and Sexual Violence" by Carolina Seigler at Princeton University, who kindly released their DMP for reuse. We have modified this plan to reflect the requirements of NIH and resources at UIUC. **This example is provided for illustrative purposes only since all Plans submitted to NIH must reflect the specific research project proposed.** See more information here: https://go.illinois.edu/newnih

---

Project Title: Religion and Sexual Violence

1. **Data Type**

This study will generate data primarily through (1) participant observations of support groups for those abused by clergy and (2) in-depth, semi-structured interviews with these individuals. Data will be collected in person or via phone calls and video calls hosted on encrypted and passcode-protected conferencing platforms.

Data will be collected in the form of digital audio recordings (collected on an external recording device free of any network connections), transcriptions of these recordings, physical notes taken during participant observation sessions, and any documents (e.g., email correspondences, scanned copies of letters or photographs) that respondents voluntarily choose to share with the researchers. All data in this study will be de-identified and associated with an anonymizing alpha-numeric code. See "Access, Distribution, or Reuse Considerations" for information on privacy and security.

It is anticipated that the data, metadata, and analysis files will together demand about 100 GB of storage and most of these data will be preserved in DOCX, JPG, MP3, PDF, PNG, TXT, CSV or XLSX format.

This study collects sensitive PII pertaining to incidents of sexual trauma. The researchers and institutional review board have determined that this study presents the highest level of risk to research participants. At this time, the researchers do not anticipate sharing interview transcripts, records, and notes with the study participants, nor do they plan to make these data available to the wider scientific community.

2. **Related Tools, Software and/or Code:**

Data will be imported into a qualitative or mixed-methods analysis software such as R or SPSS. When using this software to access and analyze data, researchers will use a password protected device in a secure location. Researchers will also produce metadata describing all collected materials as well as the alpha-numeric schema researchers will use to systematically pseudonymize any personally identifiable information (PII).

3. **Standards**

Digital audio files will be processed in MP3 format and saved as password protected files using the naming convention year, month, day, alpha- numeric pseudonym code, and approximate time of original recording. Interview transcripts will be saved as password protected DOCX files using the same naming convention. Once imported into the data analysis software they will be saved as password protected files in that software's unique format. Metadata and anonymization keys will be saved as password protected XLSX and/or CSV files.

4. **Preservation, Access, and Associated Timeline**

Given the sensitive nature of these data, it is not anticipated that researchers will utilize cloud services in this study, nor that data will be transferred during this study. All data and metadata

developed during this study will be stored on password protected and encrypted research spaces. Digital data will be accessible only through servers requiring multifactor authentication utilizing a mechanism approved by [University]. A backup of these data will be stored on an external hard drive that is password protected, free from all network connections, and kept in a locked drawer in a researcher's locked office. Physical documents acquired throughout the data collection period will be kept in a location separate from other research data in a different locked container in a researcher's locked office.

Data will be maintained on an external hard drive (password protected, free from all network connections, and kept in a locked drawer of a researcher's locked office) for a minimum of three years after the conclusion of the award.

5. Access, Distribution, or Reuse Considerations

To further protect the privacy of research subjects, researchers will not collect written documentation of consent. The [University] IRB has approved this waiver as the only record linking the subject and the research would be the informed consent form and the principal risk would be potential harm resulting from a breach of confidentiality.

To protect against unauthorized access during the virtual data collection period (includ ing but not limited to online threats, unwelcomed messages or images, harassment, or attempts to "Zoom bomb" conference calls), researchers will follow the University's guidelines to proactively ensure the security of online interview sessions. Furthermore, we have consulted with the University's Office of Privacy & Cybersecurity and incorporated their feedback in our plans.

The researchers are confident that they have put in place provisions for appropriate protection of the research subjects' privacy and confidentiality. However, given the highly sensitive nature of this study as well as the enduring ethical debates surrounding access to sensitive qualitative data, the researchers do not plan to disseminate these data for public use. A breach of confidentiality could potentially cause great psychological, emotional, or personal harm if otherwise private accounts of sexual violence were to be connected to their identity. To respect the participants' rights to be free from unreasonable intrusion, including control over the extent, timing, and circumstances of obtaining personal information about them, only the research personnel associated with this project will be granted access to these data.

Any suspected breach of PII that occurs within the context or scope of the researcher's NIH award will be reported to the appropriate offices at both [University] and the NIH. The researchers will cooperate and freely exchange information with these offices as needed to properly escalate, refer, and respond to a breach. They will together validate the scope and nature of the incident and establish an appropriate response plan.

6. Oversight of Data Management and Sharing

[Project personnel's name, title, role] will be the primary researcher tasked with collecting, reviewing, analyzing, managing, and retaining the data and the metadata for this project as well as responsible for updating and revising this Plan when necessary. Only personal included on the approved IRB application will be allowed access to the data. All personnel have past research experience with collecting and managing sensitive data, specifically data from in-depth interviews with vulnerable persons. Researchers will ensure that all research personnel have thoroughly read and understand the study protocol. All researchers have received ethics training and certification per the University guidelines.