**Data Management and Security Plan for the \_\_\_\_\_\_\_\_\_\_ Study**

Personnel:

Principal Investigator:

Co-Investigator:

Faculty Advisor:

Data Security Officer (DSO) for this project:

Research Assistants:

Training:

1. Collaborative Institutional Training Initiative (CITI) – **Basic Human Subjects Research course (required for \_\_\_\_\_\_\_)**
2. **CITI - Undergraduate Training on Human Subjects Research (required for \_\_\_\_\_\_\_)**
3. CITI optional module - “Research and HIPAA Privacy Protections (ID 14)
4. Computer login
5. Restricted Access to lab and files.
6. Research activity log - name, date and time login, list all files reviewed, logout time.
7. Research assistants will sign training acknowledgement sheet.
8. Only \_\_\_\_\_\_\_ will determine who can have access to the data files for this project.
9. Research assistants will be trained to abide by strict privacy and confidentiality parameters.

Access and Security:

The \_\_\_\_\_\_\_\_ Lab is in Room \_\_\_\_\_ of \_\_\_\_\_\_\_\_ and is controlled by a coded lock. The door code will be changed when determined to be necessary to protect data and equipment from loss. The door is locked at all times. Only authorized researchers and staff have the access code to unlock the door of the lab. Only authorized personnel may be in the lab.

\_\_\_\_\_\_\_\_\_ is the only person who can grant access to the lab and the door code. Only \_\_\_\_\_\_\_ will determine who can have access to the data files for this project.

The computer where files will be stored is password protected. Research assistants will use their University login information to unlock the computer and will be required to manually lock it when stepping away from the computer or out of the lab. The computer will also have a 10- minute auto lock activated for inactivity.

\_\_\_\_\_\_\_\_\_\_ will maintain control of the link and password (OneDrive folder or other storage device controlling access to data) containing files.

The [\_\_\_\_\_\_\_\_\_](https://rc.partners.org/news-events/presentations/dropbox-business-partners-healthcare) folder holding the files will not allow download or modification of the files. All files are encrypted in storage and in transit.

The computer used for viewing the files does not have any recording software or applications (e.g., Panopto is not installed).

No one is allowed to record video or audio or take photographs of the video files with any device.

Physical copies of the coding sheets will be stored in a locked cabinet within \_\_\_\_\_\_\_ and will be shredded at or prior to the conclusion of the project. Physical copies of the coding sheets will not contain any PHI.

Documentation:

Research assistants will sign a document assuring:

(1) they will manually lock the screen or log off from the desktop computer when stepping away or leaving the lab,

(2) they will not share any information of the participants, the files, or the content with anyone outside the research group, nor discuss data with others in the research group in public,

(3) they will not attempt to access the recording folder outside of \_\_\_\_\_\_\_\_, nor download the files on portable media such as thumb drives or portable hard drives.

Research assistants will sign up for work hours on the laboratory schedule.

Research assistants will document their activity in a log that documents their name, login date and time, files viewed, and logout time.

Research assistants will record the analysis results on paper documents and transfer the information to the electronic platform. (This statement may deleted or modified as appropriate for the project.)

Any paper documentation of analysis will be stored in a locked cabinet until the end of the project and then will be shredded.

The activity log will be reviewed periodically to ensure progress. If security anomalies occur, activity log will be compared to computer login information and file activity.

Activity log and Audit documents will be retained for a minimum of 6 years.

Project details:

1. UL Lafayette researchers are going to access files, classified as electronic Protected Health Information, and stored at \_\_\_\_\_\_\_\_\_\_\_.
2. \_\_\_\_\_\_\_\_\_ will collect the PHI and store it in \_\_\_\_\_\_\_\_.
3. \_\_\_\_\_\_\_\_\_\_\_ will provide unique access information to each person who will access the file(s).
4. Research assistants may only access the folder with the files while in the \_\_\_\_\_\_\_\_ (list an on campus space). All analysis activities will only be conducted in the \_\_\_\_\_\_\_\_\_\_. No individuals other than the authorized researchers may access the files.
5. Analysis of the data will be documented using \_\_\_\_\_\_\_\_. Participants have been assigned ID numbers. All analysis results will use the participant ID numbers to communicate the coding results.
6. Research assistants will analyze the data.
7. After completing the analysis of the data, research assistants will transfer the results on any physical analysis sheets to an online data platform hosted on \_\_\_\_\_\_\_\_ by entering the data into \_\_\_\_\_\_\_\_\_.
8. For each data analysis session, research assistants will also record in the data access log the initials of their names, the day and time of analysis, and the file they accessed.
9. Physical copies of any analysis sheets will be stored in a locked cabinet within \_\_\_\_\_\_\_ and will be shredded at or prior to the conclusion of the project.
10. Only ID numbers of participants will be used for the communication of the analysis results. As the analysis results shared by the PI will be de-identified, the results do not readily reveal identities of the participants.
11. If research assistants are aware of any data security incidents (such as the lab remains unlocked with no one inside or the computer is unlocked with no one using it) they should notify \_\_\_\_\_\_\_\_ at UL Lafayette so further actions can be taken to ensure that no data has been accessed and leaked.
12. If research assistants are discovered to be sharing data with someone outside of the lab, or to download the files to their own devices or for their own use, their involvement with the \_\_\_\_\_\_ and with this project will be terminated, and \_\_\_\_\_\_\_\_ will ensure removal of any data incorrectly possessed.
13. Should there be a need to change or modify this security plan, \_\_\_\_\_\_\_\_\_ will provide an updated data management and security plan and seek review and approval before any changes will be implemented.

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ have read and understand the requirements for maintaining security of the electronic Protected Health Information data and privacy and confidentiality of the participants in this project.

I agree to abide by these requirements and understand that \_\_\_\_\_\_\_\_\_ will have the right to remove me from the project and end my position in her lab if I violate any of the provisions in this data security plan.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature Date

I, \_\_\_\_\_\_\_\_\_ (PI or Faculty Advisor) agree to abide by the requirements of this plan, make adjustments to the plan to protect the data and participants as necessary, and assist my Research assistants with difficulties they encounter while coding of the videos to prevent loss of data or violation of privacy and confidentiality.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature Date