Example of Data Storage Policy shared by Dr. David Phillips, Assistant Professor, Exercise Science and Physical Education

Policy and Procedures for Data Storage in Research

All involved research personnel read and receive a copy of the Policy and Procedures for data storage prior to involvement in data collection. Information gathered will be kept electronically. All information will be categorized into one of two categories: name/contact information and research data. These two categories of data will not be stored in the same files. In this way, the research data will be de-identified. An encrypted and password protected linking document will be created that simply contains the name of the subject, contact information, and their subject code e.g., JPS001F. The name/contact information will be stored on the PI’s MSUfiles location. The de-identified data files will be stored and backed up using the following guidelines:

1. Numerical raw data file types.
These files are saved using the subject’s assigned code, eg. JPS001F along with a description of the type of trial. These files are generally in .csv or .txt file extensions and can be opened in Microsoft Excel for further analysis. No subject identifiable data is contained within the file. The only way to link the file to a specific subject is via the subject intake form and name/contact information file. The subject intake form is stored in PI’s office with the informed consent forms in a locked cabinet. The name/contact information file is stored in the PI’s MSUfiles location and is password protected.
The data files are stored on the password protected, data collection computer and/or the data is backed up to two password protected external hard drives housed in the exercise science laboratory. The hard drives are encrypted and password protected. The data is further backed up to Google Drive. All personnel listed in the IRB protocol will have access to these files via Google Drive. The PI monitors personnel access to the folders with sharing permissions removed upon completion of the project.
2. Video Footage.
These files are saved using the subject’s assigned code, eg. JPS001F along with a description of the type of trial. These files are generally in .mp4 file extensions and can be opened in any digital media player. The only way to link the file to a specific subject’s name is via the subject intake form and name/contact information file. The subject intake form is stored in PI’s office with the informed consent forms in a locked cabinet. The name/contact information file is stored in PI’s MSUfiles location and is password protected.
The data files are stored on the password protected, data collection computer and the data is backed up to two password protected and encrypted external hard drives housed in the exercise science laboratory. Once the data is backed up, it is deleted from the video recording device (iPod, iPad, video camera, ect). If the video files are not being actively analyzed on the data collection computer, they are deleted as storage space is limited.

External Hard Drive Policy

As research personnel may not be consistently on the MSU campus, it may be necessary to work on data offsite. In the case of video footage, they will need access to one of the external hard drives. Research personnel listed on the IRB protocol may remove one of the external hard drives for offsite use. The external hard drive is encrypted and password protected. At the conclusion of the data analysis, the hard drive is returned to the lab. All research personnel are CITI certified. If an external hard drive is destroyed/damaged/lost/stolen, an incidence report is to be filed with IRB and the drive replaced.