DATA POLICY

Purpose

The purpose of this policy is to provide researchers with the necessary information when conducting Human Subjects research and collecting confidential or private information from participants. The following defines different types of data discussed in this policy.

Types of Data

Identifiable -- any information (personal identifiable information PII) or material (such as identifiable biospecimen) that can link a participant to a research study. These are the 18 HIPAA identifiers that are considered personally identifiable information.

Anonymous – The dataset does not contain any identifiable information and there is no way to link the information back to identifiable information.

De-identified – The dataset does not contain any identifiable information, but there is a way to link the information back to identifiable information.

Confidential -- PII that a participant may not want anyone to obtain without their permission. This may include, social security number, phone numbers of friends/family/colleagues/students, or driver's license numbers.

Coded-- Data are coded when a link will exist between a unique code and PII such as name, medical record number, email address or telephone number.

Protected Health Information (PHI) -- any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

Private Information -- includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public.

Data Storage & Data Sharing

Data storage is long term storage of any data collected from participants. Data sharing includes granting access to any data to multiple researchers. Below are types of storage.

Types of Storage

Desk-top & Lap-top Computers

University owned computers are preferred over personal as they are protected by multiple factor identification. Regardless of whether the computer is University owned or personally owned, it is expected that the devices and data will be password protected and kept in a secure location (such as a locked office).

Thumb Drives & External Hard Drives

Thumb drives are only approved to use when conducting field work and must be encrypted. The preferred storage is the CSUB Cloud drive, lap-top, or computer hard-drive.

Cloud Storage

The CSUB HSIRB only approves the use of CSUB Cloud Drives such as Box and Google Docs.

Zoom Recording, Transcription, and Storage

Zoom recordings may either be recorded to the researcher's laptop/computer or the Zoom Cloud; however, be aware Zoom Cloud storage is only temporary. Zoom cloud storage is only retained for approximately 6 months. An alternative would be to have the Zoom cloud recording uploaded to CSUB's Panopto and saved there until the recordings are destroyed. Transcriptions may be shared with the participants for checking only in person or through CSUB Box or Google drives. No transcriptions may be shared over email. Transcription services should be chosen from the approved list of transcription services, or the link to the service's data security should be included in the protocol for approval.

Audio & Visual Recording Devices

On recording devices, handheld or digital recorder, tape-recorder, or laptop computer designated for research purposes are allowed; cellphones are not an option. Personal cellphones are carried around in public places and are more likely to be lost or accessed by others.