School of Education Human Subjects Research
Data Security and Storage Guidelines

The security of data varies depending on the type of data and the risks associated with breach of data security. In the following chart, these codes are used:

ID = data that include personal identifiers (name, DOB, class, school, etc.) or the identity of the participant could be deduced

NID = data that does NOT include personal identifiers

Category	Examples/Types	During data collection and analysis
Consent forms Assent forms		Secured, originals on campus as soon as possible; separate from other data and file linking names and id numbers/pseudonyms (electronic folder or file cabinet)
File linking names with id numbers or pseudonyms	Paper	Secured in locked file cabinet stored in locked office; stored on campus as soon as possible
	Electronic	Encrypted on CEHD server; in separate electronic folder than other research data files
Assessments (pre and post data), testing protocols, work samples	Paper data (tests, materials)	Secured in locked file cabinet stored in locked office (on campus as soon as possible)
	Electronic data (Excel, SPSS, SAS data)	ID– on CEHD server, encrypted NID– on password protected system
Filed Notes, Journals	Paper	Secured in locked file cabinet stored in locked office (on campus as soon as possible)
	Electronic	ID– on CEHD server, encrypted NID– on password protected system
Audio-recordings	Tapes	Secured in locked file cabinet stored in locked office; these can be destroyed as soon as transcribed
	Electronic file (audio)	ID - on CEHD server, encrypted NID – on password protected system
	Transcripts (paper)	Secured in locked file cabinet stored in locked office
	Transcripts (electronic)	ID - on CEHD server, encrypted NID – on password protected system with care to ensure any sensitive information
Video-recordings	Tapes, electronic file	ID – on CEHD server, encrypted Secured in locked file cabinet stored in locked office ; these can be destroyed as soon as transcribed
	Transcripts	ID – on CEHD server, encrypted NID – on password protected system with care to ensure any sensitive information
Pictures		ID – on CEHD server, encrypted
Data sets (electronic)		ID – on CEHD server, encrypted

		NID – on password protected system with care to ensure any
Survey data	Paper copies	Secured in locked file cabinet, stored in locked office
	Electronic copes	ID – on CEHD server, encrypted NID – on password protected system with care to ensure any sensitive information
	Qualtrics	Qualtrics server
Other electronic data (web)		Password protected access only

Notes:
1. Sakai is also considered a secure server, but may not have sufficient backup systems in place in case of a server "crash". Consult with Office of Information Technologies on campus for more information.
2. Flash drives and external hard drives are less secure options for storage of data given possible loss or theft. Researcher should put in place adequate protections for research records that are temporarily stored on portable devices (password protected, encryption). External hard drives that are used for data storage should be locked in file cabinets or other locked location. Data with any identifiers should not be stored on any portable storage device.
3. Any sensitive data that is sent through email should be encrypted.

Availability of Research Records for Open Projects

A copy of research records should be available on campus. This includes the original or a copy of the consent forms and one complete set of research data. Data can be in one form. For example, the audio recording of an interview OR the interview transcript should be available; both are not required.

Storage of Data on CEHD/OET Server

Faculty and students have access to CEHD/SOE Server for storage of human subjects and related research. Off campus access is available through VPN. To apply for an OET user account, the faculty member should write to oet-help@udel.edu to request an account. If the request is for a student account, the faculty advisor should request the account through oet-hep@udel.edu and copy the student on the e-mail with the student's UD e-mail address. It is important to indicate whether or not faculty advisor would have access to student OET files. Faculty advisors should indicate (by writing to oet-help@udel.edu) when data and records on the CEHD/SOE server can be deleted.

Data Storage After Research is Complete (Closed Projects)

A copy of research records (e.g., consents, data, approval for initial protocol, amendments, continuing review) must be available for 3 years following the close of the project and available on campus. Original copies of consent/assent forms should be retained on campus. Records can be sent to the Research Office to be stored in University archives.

Data Storage for Projects of Faculty or Students Who Leave UD

A copy of research records (e.g., consents, data, approval for initial protocol, amendments, continuing review) must be available for 3 years following the close of the project and available on campus. Original copies of consent/assent forms should be retained on campus. Faculty advisors (or other supervisors) are responsible for storing data records or data records can be sent to the University Archives for storage. Records sent to the University Archives can be labeled with a "destroy by" date, if appropriate. For example, if the project ended on 10/1/12, then the "destroy by" date could stipulate that the research records for the project could be destroyed on or after 10/1/15.

Students or faculty members who leave UD and take a copy of the data with them are responsible for maintaining the same levels of data security. As soon as possible and to the extent possible, the file linking names to id numbers/pseudonyms should be destroyed and all identifiers removed from research records.