Research Data Security & Management

Research data may be collected in many ways (i.e., questionnaires, audio/video tape, online surveys). Additionally, the data may be stored in a range of formats (i.e., handwritten notes, analog/digital recordings, computer files). Each mechanism for collection and storing data poses particular issues with regard to security against unauthorized access and use, prevention of accidental loss or damage, and eventual disposal. Maintaining human subject data securely with the appropriate level of anonymity, confidentiality, or de-identification is a key factor in minimizing the risk for research participants, the researchers, and the university.

Best Practices for Data Security Recommended by the IRB and the Office of Information Technology

- All electronic data collection and storage devices should be password protected with a strong password. A strong password requires a level of complexity. Please visit the Office of Information Technology (OIT) password site for additional information.
- If it is necessary to use portable devices for the initial collection of identifiers, the data files should be encrypted and the identifiers moved to a secure system as soon as possible. The portable device(s) should be locked in a secure location when not in use. All data collected on a portable devices should be transferred to an approved platform as soon as possible after collection and deleted from the portable device.
- Access to identifiable data should be limited to members of the research team.
- Identifiers, data, and keys should be placed in separate, password protected/encrypted files and each file should be stored in a different secure location.
- Ensure that you are storing and/or transmitting files on an approved platform.
- Remove all direct identifiers as soon as possible, possibly using codes in lieu of the identifiers.
- Use accepted practices to protect against indirect identification, such as aggregate reporting or pseudonyms.
- Ensure that the research data, when destroyed, is done so in a manner that protects the participants. Hard copies of the data should be shredded and electronic data files should be deleted from all storage devices including any recycle bins. OIT has resources for helping with remediation of electronic data to learn more visit UCCS IT.

Key Definitions

The UCCS often finds incorrect use of anonymous, confidential, and de-identified. Understanding the correct use of these terms can assist in determining appropriate data management and security for the protocol.

- *Anonymous Data:* Data originally collected without identifiers. Data are anonymous if no one, including the researcher, can connect the data to an individual. No identifying information is collected from the participant. Be aware that the collection of indirect identifiers (i.e., information regarding other unique characteristics) might make it possible to identify an individual from a pool of subjects. For example, a participant that is a member of a minority ethnic group might be identifiable from the pool of subjects.

- *Confidential data:* A link between the data and the individual that provided the data exist. The research team is obligated to protect the data from disclosure outside the research according to the terms of the research protocol and informed consent document. The best defense against a breach of confidentiality is multiple layers of security.

- *De-identified data:* Although collected in an identifiable manner, any direct or indirect identifiers or codes linking the data to the individual participants are removed and destroyed.