UNF IRB Guidance on Secure Data Storage

When researchers collect data that could be identifiable, there are minimal data security standards to which all researchers must comply. When data are sensitive, additional security controls such as encryption may be required. Please see the following pages for more information about data security standards and options. If you have questions, please contact a research integrity administrator by calling (904) 620-2455 or emailing irb@unf.edu.
Required minimum data security standards when collecting identifiable information:

Failure to comply with the data security standards outlined in this document could result in increased risk to participants. If you are completing a UNF IRB application, please outline (In the Attachment A document, section #9b: Data Storage, Security, and Monitoring section) how you will comply with the data security standards outlined in this document. Please provide as much detail as possible in your application about data security to minimize the chance that you will be asked to provide additional information at a later date.

1. All data collection and storage devices must be password protected with a strong password. A strong password is long and not easily guessable. For more information about setting good passwords, please see the password guidance webpage on the UNF IT Security website.

2. Identifiers (including signed informed consent documents), data, and master lists (i.e., documents connecting pseudonyms/codes with identifiers) should be stored in separate and secure locations from each other. By storing this information separately, the risk of a breach of confidentiality is lessened.

3. Identifiable information should not be stored on portable devices (e.g., laptops, tablets/smart phones*, USB/flash drives) when it can be avoided. However, if it is necessary to use portable devices for storing identifiable information, the data files must be encrypted. Portable devices should also be locked in a secure location when not in use. Please contact a research integrity administrator or UNF IT security personnel to discuss your options for encryption. For example, PCs have a built-in encryption software called BitLocker that can be used to encrypt drives, USB/flash drives etc. Macs have their own built-in encryption software called FileVault. Please contact the UNF IT department for more information about how to use these tools or other encryption options. Please note that any identifiers collected must be moved to a more secure location as soon as possible.

4. You may request access to dedicated storage space on a UNF secure server for your research. Requests for access to secure storage should originate from faculty or research integrity staff members. Students will need their faculty advisors to request space on their behalf. Faculty and staff who are interested in receiving access to secure server space will need to email their CTECHs in the UNF IT department and copy research integrity at irb@unf.edu. Within the email please
   • Indicate that you or your student requires secure server space to ensure human subject research data are secure
   • Provide N numbers for all individuals for which you request secure server access. This will allow for easy access by IT staff.
   • Provide an estimate of the amount space needed (if you are unsure, please describe the data that will be stored (e.g., 3 90-minute focus group audio recordings and transcriptions)
   • Finally, estimate how long you and your personnel will need data to be stored in that location (e.g., 60 days for audio recordings and an additional 90 days for transcriptions at which time transcriptions will be moved to another location).

5. Please do not send identifiable private information through regular electronic mail (E-mail) as it is not secure. For more information about securely transferring sensitive data, please meet with a UNF IT security specialist.

*Data stored on iPads are not secure and do not meet data security standards without robust encryption. Even with encryption, iPads should be used as rarely as possible. If you are considering using an iPad, please arrange a meeting with a UNF IT security specialist.