**Guidance for Researchers: Data Security**

The safeguarding of human subjects is of paramount importance to the UCM Institutional Review Board (IRB) as the IRB is charged with protecting human subjects and their private identifiable information. Human subjects’ data stored on computers in text, photo, video, or other formats can be compromised through theft or hacking, and subjects may be put at risk of harm from a data breach.

In addition to the risk to subjects, the cost of reproducing, restoring, or replacing stolen or lost data highlights the need for a comprehensive data protection plan. Researchers should specifically address how they will safeguard human subject data stored in electronic and non-electronic formats in their study submissions.

**Protection of Electronic Data**

Theft and hacking are concerns with electronic data. Many research studies involve the collection and maintenance of human subjects’ data that could become the target of hackers. The following precautionary measures are recommended when dealing with electronic data:

1. Consider study goals and risk levels in the planning stages of your research study. Careful consideration should be given to the type of data needed to achieve the study aims. As the level of risk increases (depending on the type of questions being asked, etc.), so will the investigator’s responsibility for protecting study subjects’ information. Things to consider include:
* whether factors may limit your ability to securely protect human subjects research data (i.e., international travel, budget), in which case you may want to utilize written documentation or field notes that do not include identifiers.
* if using audio/videorecording, the protocol will need to describe how the recordings will be coded to protect the subject’s identity, how the recordings will be maintained (i.e., where they will be kept), and when/if they will be destroyed.
1. Securely delete sensitive data and personally identifiable subject information when it is no longer needed. Shred any hard-copy forms as soon as possible.
2. Human subjects research data files should be password protected and encrypted. Encryption reduces the risks associated with stored private information. Unencrypted data should never be emailed or otherwise shared.
3. Ensure that you follow the UC and UCM OIT [minimum-security standard.](https://security.ucop.edu/files/documents/policies/minimum-security-standard.pdf)

Devices involved with the processing data should:

* have FireEye HX installed
* are encrypted
* managed for patch and fixes
* have Crashplan cloud storage

If you are unsure if you are following the minimum-security standards or if you are unsure if your device security standards, reach out to UCM OIT for a [Research Data Security Assurance Consultation.](https://it.ucmerced.edu/content/research-data-security-assurance-consultation)

1. Restrict access to data. Be sure you know who has access to folders before you put restricted data there. Don’t put sensitive information in locations that are publicly accessible from the internet.
2. When using an online data collection site (e.g., Amazon Mechanical Turk, Qualtrics, etc.), researchers should carefully review the site’s data security policy. If the site stores identifiable information and/or links survey responses to individual participants, this must be made clear in the Protocol submission and in the corresponding informed consent document(s).