IRB Data Security Guidance Document

During the review process the IRB will consider human subject privacy and confidentiality, including HIPAA related issues. The protection of the personal and confidential information provided by participants is of extreme importance.

Specifically, in the *Procedures to Maintain Confidentiality* section of the IRB Application, PIs must:

1. Describe procedures (including safeguards for collecting, storing, processing subject data and data destruction) for minimizing potential risks to subject's confidentiality
2. Specify where and under what conditions individuals will have access to the data, what will be available and to whom.

Please consider the following when preparing your IRB application:

1. Review University of Denver UTS Guidance and Policies (http://www.du.edu/uts/policies/index.html) website for additional recommendations on how to best secure confidential data according to Institutional policies.
2. The IRB expects researchers to access only data that are necessary to conduct the study. Collect only the minimum necessary information. Social security number and full birthdate (mo/day/year) are protected information that generally should not be collected.
3. In the Informed consent document, PIs must describe protection and confidentiality of records.
4. Keep data at a secure location. A secure location is a place to which only the PI and authorized research staff have access.
5. Limit electronic access to any computer that contains subject identifiers by password protection. Avoid storing data on portable devices as these devices are susceptible to loss or theft. If the PI needs to use these devices, remove identifiers from data files and associate them with codes kept in a separate location. The data should be encrypted.
6. Remove/destroy subject identifiers as soon as they are no longer needed.
7. If participant identifiers are required for the research study, then additional justification must be provided.
8. Use only secure modes of transmission of data; data submitted over a public network should be encrypted.
9. If there is an unanticipated breach of confidentiality of the research data, the PI must report this to the IRB via eprotocol within 30 days of becoming aware of the event.

This document provides guidance on data security resources and the minimal standards for the collection, storage, use and transmission of identifiers associated with research data or specimens.