Methods for Research Data Security at the Zablocki VAMC

1. Hard copies of identified VA human studies research data must be stored in locked filing cabinets and should not leave this medical center. If there is a very good reason for removing these files, a formal request should be submitted to the ACOS/R&D, who will forward the request to the ISO. The safer method would be to scan the paper copy into a computer file and then encrypt the data. Confer with the ISO.

2. If you can store your VA human studies research data on the Zablocki VA server, it should be left there and not downloaded to other computers or portable media. The VA server is a secure device, and no additional data encryption is needed. The only VA approved thumbdrives for data storage are encrypted Ironkey drives available only through IRM.

3. If you use or store human studies or sensitive animal data on any other computer system at any location (VA research labs, FMLH, MCW, home or other locations), password protect your computer, activate a timed lockout and required password to wake it up, and obtain encryption software from Research. For PCs, the software to encrypt computer devices is called Pointsec. For Mac users, the encryption program is called Knox, which currently encrypts files instead of devices. A new version will be out soon that will encrypt devices. You will be notified when it is available.

4. If you have to send hard copies of your research data to another location, such as in a cooperative multi-site study, use a courier system such as FedEx to ensure a documented chain of custody. If you are sending computerized data, it must be encrypted such that only those authorized users identified in your project registration will have access. You can apply for PKI email encryption through the medical center.

Copies may be faxed under the following conditions:
   a. The fax number is verified before faxing.
   b. It is ensured that the information was sent to the proper destination either by direct communication with the recipient or by checking the confirmation slip.
   c. Someone is there to receive the fax or the fax machine is in a secure location (e.g., locked room).
   d. A confidentiality statement is on the cover page instructing the recipient to notify the sender if the fax is received in error.

5. **Investigators with active VA research projects involving human subjects must currently retain ALL original research data, including identifiers, indefinitely until further notice.** When the moratorium on data destruction ends, this medical center will follow the MCW data storage policy that original data must be retained for at least 10 years from the date of the last entry in the record of the last subject enrolled in the study unless mandated to be kept longer by the FDA or the study sponsor. You must ensure that this data is stored securely at Zablocki VAMC or at a storage facility approved by this medical center even if you leave this medical center, MCW or the VA.

The original research consent form must be stored for 75 years. Patient consent forms scanned into CPRS meet this requirement. For non-patient study participants, contact the Director of Research Operations in the Research Service Office for suggestions on data storage.

At the conclusion of your study, destroy any copies of the research data not needed for archival purposes. Hard copies should be shredded to particle size of 1 mm by 5 mm. If the data is on computer hard drives or portable storage devices used with the VA, the data must be overwritten. Contact the ISO for assistance in ensuring overwriting procedures meet VA requirements. If the data is on CD or other portable storage medium, the medium must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded, all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm$^2$). Electronic storage media may also be turned in to the ISO for appropriate disposal.