

Instructions for Securing and Archiving Research Data

Securing Records:

Hard-Copy research records must be kept in a secured location following standard VA practices. Generally, records containing PII/PHI or other sensitive information should be kept in a locked drawer in a locked room, and should never be left unattended. Records that are being discarded (e.g. after making a digital copy) must be placed into Shred-It bins for secure destruction.

Electronic records must be saved to the VA network, with access to the specific folder limited through use of folder permissions as follows:

STEP 1 – When creating a folder for storage of research data:

1. Create a folder on [R:\Data\](#)
2. Name the folder using the IRB/SRS/IACUC/R&D Committee number, e.g. "1234-A"
3. Use the YourIT shortcut on your VA desktop to submit a Help Desk ticket. Your ticket should request a Secure Distribution Group (SDG) to limit who can access this folder. You will need to include the following information in your request:
 - a. Indicate the NAME and PATH of the folder (e.g. "R:\Research_Data\1234-A")
 - b. Specify the NAME of the SDG (Should match the folder name for study data - e.g. "1234-A")
 - c. Include the FULL NAME of each person who should be a "group owner", i.e. persons able to add or remove group members (e.g. PI and study coordinator or lab tech)

NOTE: For files that are (a) not part of an active study or (b) from a study not involving PHI/PII (e.g. rodent or laboratory-only studies), it is OK to create one SDG for an entire lab group – **but for studies involving PHI/PII, you should create a study-specific SDG containing ONLY personnel who are named on the study protocol.**

STEP 2 – Once the Security Group has been created, the SDG owner(s) can add or remove access to the folder by adding or removing members in the SDG.

1. Click on the "MIN – GUI Executables" icon on your desktop or navigate to the network folder [\\v23.med.va.gov\apps\Goldstar\MIN\](#)
2. Open the "MIN Shortcuts" folder.
3. Locate the shortcut "Distribution Group Update", and click to open.
4. This will open the search box "Find Users, Contacts, and Groups".
5. In the search tab, enter the name of the Secure Distribution Group (SDG). Once you have located it in the list, right click on the SDG and choose the "Properties" option in the drop-down list.
6. From here you can Add/Remove members and/or see who is already a member of the list. If you cannot make changes to the selected group, you may not have permission to do so: Contact Research ADPACs for assistance.

Archiving Records:

ALL RECORDS must be maintained for a minimum of 6 fiscal years post-study closure per National Archiving & Records Administration guidelines.

Electronic and hard copy records containing PHI/PII cannot be retained by the investigator, and must be turned in to the Research Office for sequestration and long-term archiving per Federal records retention guidelines and local SOPs.

For records that do NOT contain PHI/PII or other sensitive information, investigators may retain a copy of the records provided that s/he provide an administrative copy for long-term archiving.

For data turned in either for sequestration or long-term archiving, the following procedures must be observed:

Hard copy records must be placed into archive boxes, and **MUST** include an inventory sheet describing the contents of each archive box. Contact the Research records liaison for assistance.

Electronic records must be turned in to the Research Office. Records may be turned in on VA-approved secure media (e.g., encrypted CD/DVD or VA-approved USB drive), or placed into a network folder ([R:\Data\00 ArchiveData](#)) for archiving. CCDOR projects can be archived by working with your CCDOR data team to have the electronic data moved to “projects_HOLD” folder within the [R:\CCDOR Data](#) folder.

- **If using the network folder, ALL RECORDS must be placed into a subfolder using the protocol number as the folder name.**

By placing documents in the required location(s), you are attesting that no other copies of PHI/PII are retained in the possession of the investigator.

Administrative Oversight:

The Research Information Protection & Security working group will perform a quarterly check to ensure that closed studies have followed the procedures outlined above. Studies for which procedures have not been followed may result in referral to the Research & Development Committee for failure to adhere to administrative expectations per R&D SOP 004 “MVAHCS Research Investigator Responsibilities”.