Guide to Developing a Research Data Safety Plan
(section 12.1 in eIRB)

Current best research practice at DUHS, based on guidance from the Information Security Office requires that all electronic study data be backed up on a secure, DHTS-maintained file server ("shared drive"). These shared drives can also be used as the primary repository for study data, allowing several study team members to update, work on, and maintain the same copy of the study data.

This document serves as a guide for developing a compliant Research Data Safety Plan (RDSP) (using a shared drive) and documenting the RDSP in the eIRB application.

1) Create eIRB application for the particular study. Section 12.1 will ask several questions regarding the RDSP and whether it is compliant with current DUHS policies.

2) Check to ensure that "yes' or "no" is selected for each dropdown option in the section 01. Storage Media Types.

   Any yes selection will determine what sections come next

3) PHI is almost always selected in section 02.1 Storage of Paper or Non-digital Media

   Specify the location where paper or non-digital media will be stored: ensure there is enough information to allow someone to locate the documents based on description, including room number(s) and building name(s)

   Specify who has access to the paper or non-digital media: ensure the description includes both (1) who has permission to access and (2) who has physical access (e.g. keys, swipe cards), e.g. job titles, research roles, or persons' names.

   Specify how the paper or non-digital media are secured: ensure the location of the keys is documented and how the keys are accessed. Ensure keys to storage locations are NOT stored in an unlocked desk drawer. If swipe cards (Duke IDs) are used for access secured storage, ensure a list of whose cards work in that access device can be obtained. The study team does not need to maintain the list themselves, but they should know where to locate the list. *Study data that includes **Social Security Numbers require "two keys" for paper storage. This could be a swipe card to access the floor/unit and a locked file, locked office and file, etc.***

4) PHI is almost always selected in section 02.2 Storage of Electronic Information
   At least one entry is selected to describe who is managing the infrastructure.
   Duke Medicine Managed IT Service is **not** selected.

5) Section 03. Duke Electronic Storage Details

Data is stored within a folder on one or more Duke file servers: Yes Always answer yes.

The shared drive must be set up by IT support staff. This can be initiated by placing a Help Desk <https://duke.service-now.com/navpage.do>ticket with the subject "Need shared drive created for research". You should also send an e-mail to Joyce Owens with DHTS to make sure that she is aware, since these requests are sometimes not routed to her correctly. You can store your data on your private drive/DUHS-approved encrypted computer or mobile device, but a shared drive backup must also be created.

Example:\\duhsnas-pri\duhs_radiology\private\research
File within the share drive name example: PI Name _research.
File within the primary file name example specific Pro000…
Fitzpatrick East Data Center (this is where the Radiology server is located)

Once the shared drive is created, you can create multiple folders within the drive, one folder per IRB-approved research project. You can then manage the "permissions" associated with these folders to make sure that the study team members can see the right folders, but not the folders for projects with which they are not involved. Changing folder permissions requires placing a ticket with the DHTS Help Desk with the subject "Need to remove/add <name > from shared drive <name>; you should again follow up with Joyce Owens if these requests are not fulfilled within 1-2 days.

6) Section 04. Software Environment & Survey Tools

The entity responsible for managing the software / database / website:
Use DHTS, 684-2243 if you are unsure.