# Data Management Plan for Projects with PHI on HiPerGator

V1 May 9, 2023

The users and their project supervisors/mentors are responsible for ensuring that the endpoints used to access HiPerGator follow UF standards:

* Encrypted laptops
* Screen lock after 15 minutes of inactivity
* Use devices in locations where shoulder surfing is not possible

The responsibility of the Principal Investigator of the project includes

* Provide instructions to users for when they telework from approved locations to ensure that these procedures are followed.
* Instruct users to not access the HiPerGator system and their PHI projects from their endpoints while in public locations like airports, libraries, and venues like Starbucks.
* Instruct users to not copy restricted data from the designated storage area in HiPerGator
	+ To their endpoint (desktop, laptop, other server, mobile device).
	+ To any other storage location in HiPerGator accessible to the user (home directory, other shared folder the user has access to).
* Designate a data manager, whose responsibility includes
	+ Record and maintain the signed data management plan form (paper or electronic) signed by each user after training.
* Reconcile the list of authorized participants with that maintained in the IRB record.
* Keep a record of when users complete training and ensure that training is renewed annually or as needed.
* Verify and review authorized accounts regularly, at least once per month, and notify RC staff immediately when users leave the project, change roles in the project (e.g. when they take on a new job in the university or leave the university) so that access to the PHI project can be removed promptly.
* If the PHI project involves transaction-based systems, the project manager and team are responsible for ensuring transactions can be recovered in the case of failures. This can be implemented in collaboration with UFIT Research Computing staff.
* If there are special precautions that apply to this project and are called out in the risk assessment, then such actions or requirements will be added to the agreement documented in Archer and become part of regular review, vulnerability scanning, and/or risk assessments, depending on the level of risk assessed for the set of special precautions.

Name: Date:

Signature: