Allowable Storage, Required Backup, and Temporary and Off Campus Storage Options for Digital Research Data

Research Data Category	Security Risk	Allowable Data Storage Options	Required Data Backup Options	Allowable Temporary and Off-Campus Storage Options
I. HIPAA Research Data, and master lists with HIPAA identifiers.	High.	• HIPAA compliant ETSU network drive[1]; or • ETSU HIPAA REDCap[3]; or • ETSU AWS account within the HIPAA Perimeter[4]; or • Hospital or clinic EHR System.	Backup is automatic with all allowable data storage options.	• HIPAA compliant ETSU network drive[1] • ETSU-owned encrypted devices.[2] • ETSU HIPAA REDCap[3] can be accessed from off campus. • ETSU AWS accounts within the HIPAA Perimeter[4] can be accessed from off campus.

II. Non-HIPAA Identifiable Human Subject Research Data, including but not limited to FERPA Research Data and Master Lists for non-HIPAA Coded Human Subjects Data.	High; for Coded Research Data, the master list must be stored securely but separately from the de-identified coded data.	• ETSU network drive[5] (automatic backup); or
		• ETSU OneDrive for Business (automatic backup); or
		• ETSU REDCap[3] (automatic backup); or
		• ETSU desktop; or
		• ETSU encrypted laptop, tablet, or external drive; or
		• ACF[4]; or
		• AWS[4].
			• ETSU network drive[5]; or
			• ETSU OneDrive for Business; or
			• ETSU REDCap[3]
				• ETSU-owned encrypted devices.
				• The following can be accessed from off campus:
				  ○ ETSU OneDrive for Business
				  ○ ETSU REDCap[3]
				  ○ ACF[4]
				  ○ AWS[4]

III. Non-Human Research Data, Unidentifiable Human Subject Research Data, and Appropriately De-Identified Coded or Non-Coded Human Subject Research Data.	Low-Moderate. For coded data to be allowed under this category, the master list must be stored separately (under category b storage) from the coded de-identified data.	At the discretion of the researcher.	• ETSU network drive[5]; or • ETSU OneDrive for Business; or • ETSU REDCap[3].	At the discretion of the researcher.

Special Note: See Data Storage Policy for information regarding collaborative studies

1. PI's who require access to the HIPAA network drive must contact the HIPAA Compliance Officer; HIPAA@etsu.edu.
2. PI's who require use of an encrypted flash drive for temporary storage may personally purchase a new encrypted flash drive and comply with this section so long as the encrypted flash drive is only used for the research study.

3. For access to the HIPAA REDCap or REDCap server, please use the Computer Account Request and Access Form on the ITS Forms Page. Information about REDCap is available on the ITS website.
4. If you require access to ACF or AWS for advanced computing, please contact Vincent Thompson, 423.439.4492.
5. PI's who require a shared folder on the S: drive or T: drive should submit the Computer Account Request and Access Form found on the ITS Forms Page and use section 4 of the form to identify the project and names and ETSU e-mail addresses of staff who require access.
6. OneDrive resources are at the bottom of the 365 Users page.