IRBNews

New Data Storage & Backup Policies

Information Technology Services (ITS) has created a policy for researchers regarding how to properly handle their research data. These guidelines define backup, categories of data, encryption of data, and data storage.

ITS has defined appropriate locations for the storage and backup of research data. Some general principles about data storage and backup instructions are as follows:

First, all researchers, including student researchers under their advisor's supervision, share the responsibility for storage and backup of research data.

Second, the appropriate storage and backup locations vary depending of the category of data. For example, if the data is subject to HIPAA rules, there are stricter requirements for data storage. This new policy outlines acceptable storage and backup locations for the different categories of data.

Third, principal investigators are responsible for ensuring that their proposed data storage, backup methods, and storage location comply with this policy. Before you submit your study to the IRB, please be sure that you read and understand this policy. In your New Protocol Submission xForm, be sure that your proposed methods are compliant with this policy, and be sure that you clearly explain your data storage, back up methods, and location to the IRB. This will help prevent delays in the review and approval process. As you carry out your study, be sure that you do so in accordance with methods entered in the IRB approved protocol and this policy.

Lastly, be sure that your study data is stored for the required period in accordance with the IRB approved protocol and this policy.

Guidelines Specific to Student Researchers:

- Student researchers must provide copies of their research data to their research supervisors at intervals determined by the supervisor and at the conclusion of the study.

- The research supervisor or designee is responsible for the storage and backup of data for a period of 6 (six) years from the end of the calendar year in which the study is closed or for the requisite time period specified by the research sponsor or other regulators, whichever is longer.

A helpful chart is included with the policy under the **Related Forms** section. This chart specifies the different categories of data and how that data should be handled. The Digital Research Data Storage and Backup policy and the attachments can be found within the University Policies web page under Information Technology

Contact Information:

For questions about this policy, contact the Director of Research Computing – David Currie, currie@etsu.edu, (423) 439-6457

For questions about HIPAA data, contact the HIPAA Compliance Officer – Lindsay Daniel, daniell@etsu.edu, (423) 439-8533

EAST TENNESSEE STATE UNIVERSITY