Digital Research Data Storage and Backup Policy Draft	
Responsible Official: Dr. William R. Duncan	Responsible Office: Office of Research and Sponsored Programs

Policy Purpose

This policy promotes secure and reliable means to store and back up digital research data using the East Tennessee State University (ETSU) network or ETSU-approved cloud solutions. The policy reduces the odds of data loss or inappropriate release of sensitive data through accidental means, mechanical failure, or malicious activity and may reduce overall purchases of incidental hardware storage devices. ETSU and its researchers share in the responsibility to secure and protect regulated and other sensitive research data. Failure to do so may result in severe penalties levied against individuals and the institution. ETSU's Chief Research Officer or the ETSU IRB committee chairs may require access to research data in order to protect intellectual property rights, to fulfill requirements to research sponsors, to protect against charges of academic misconduct, to assure compliance with regulations protecting human and animal subjects of research, to assure safe use of potentially hazardous research materials or products, and to safeguard regulated data.

Policy Statement

Faculty, Staff, and Student Researchers at ETSU must meet or exceed the safeguards and standards as outlined in the procedures for digital research data storage and backup. All procedures related to human subject research data are subject to ETSU IRB approval.

Authority: (Statute, regulation, THEC policy, Executive order, or other authority governing the policy)

I. **Legal:** The collective acts identified as Export Control Regulations ("ECR") administered by federal agencies including but not limited to the Departments of State, Commerce, Treasury, Defense, Energy and U.S. Customs; the Family Educational Rights and Privacy Act (FERPA); the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH Act"), as set forth in Title 45, Part 46 (Protection of Human subjects), Subpart A (the "Common Rule"), Parts 160 through 164 (the "Privacy Rules", the "Security Rules", the "Breach Notification Rules", and the "Enforcement Rules") of the Code of Federal Regulations (collectively, "HIPAA"); the Tennessee Data Disposal Regulation Tenn. Code Ann. § 39-14-150; various regulations within the Tennessee Financial Records Privacy Act Tenn. Code Ann. § 45-10-*

II. **Institutional:** ETSU's Office of Research and Sponsored Programs (ORSP) oversees the review and management of all funded and unfunded research at ETSU. The ETSU Medical Institutional Review Board (IRB) Chair and Campus IRB Chair and their respective committee members must approve of all studies involving human subject data. The ETSU HIPAA Compliance Office must approve of data handling and other procedures for studies involving HIPAA regulated data and control of access to protected health information (PHI). The University Committee on Animal Care oversees the use and care of animals in research activities. The ETSU Export Control Compliance Officer within the ORSP must approve of data handling and other procedures for export controlled research or research data subject to Export Control Regulations. The ETSU Office of the Registrar determines and controls access to data regulated by the Family Educational Rights and Privacy Act (FERPA). The Office of Institutional Research controls access to institutional data. The Office of the Bursar controls access to financial data. The ETSU Office of University Counsel is available to assist with interpretation and compliance in all matters relating to the handling of data subject to regulation, control, or restricted access or considered sensitive or confidential.

III. **Collaborative Studies:** When ETSU researchers collaborate with other institutions, they should consult with the ETSU IRB to coordinate approval between institutions. While the primary IRB is that of the institution with primary ownership of the data, the data plan must generally meet the data security requirements of both institutions. Sharing of human subject data with external collaborators or investigators via ETSU resources requires approval of the ETSU IRB.

IV. **Data Use Agreement:** Data use agreements (DUAs) may have additional restrictions about storage of data. Data use agreements must be routed through the Vice Provost for Research for review and signature. The ETSU IRB must be informed if a data use agreement applies to the research. The recipient of the data is responsible for ensuring that the data storage meets the restrictions of the DUA.

Definitions

- **Data Backup:** Data Backup refers to a secondary location to which data files are copied and from which data files can be retrieved in the event that data files in the initial storage location unexpectedly become unavailable. Backup should be done as often as possible.
- **Data Categories:**
    - Coded Research Data: Coded research data is a de-identified dataset that is tagged with a robust code (such as a random number). The code is also tagged to an identifier list (master list) and/or to a dataset containing identifiers. In summary, coded datasets are created through appropriate de-identification of identifiable data, but are tagged with a code that is separately linked to the identifiers. The master list to the code makes it possible to link the coded de-identified data back to the identities of individuals. The code should not contain recognizable portions of identifiers. Storage locations for the original identified data, the master list and the de-identified coded data itself must all be approved by the ETSU IRB.
    - De-identified Research Data: A dataset from which any information that could potentially be used to identify human research subjects has been thoroughly removed as approved by the ETSU IRB. De-identification makes the data suitable for public sharing, presentation, or publication. Researchers must adhere, throughout the study, to the same stringent de-identification standard initially approved by the ETSU IRB.
    - Export Controlled Information: Any information or item (including technology, technical data, software, encryption code) that cannot be released (i.e.,

accessed, disclosed, disseminated, shared, transferred) to a foreign country, or to foreign nationals or representatives of a foreign entity, without first obtaining approval or license from the cognizant Federal Agency.

    - Identifiable Human Research Data: Any regulated (e.g. HIPAA/FERPA) or unregulated dataset containing information which could be used to identify an individual. The data are sensitive but the level of sensitivity (potential for embarrassment or harm) varies with the nature of the data.
        - FERPA Research Data: Sensitive research data that include the use of a student's educational record.
        - HIPAA Research Data: Sensitive research data that include identifiable human subject data collected or created in conjunction with a HIPAA covered research study as determined by the ETSU IRB.
        - Other Sensitive Human Subject Data: Research data containing identifiers not covered by HIPAA or FERPA. The level of sensitivity varies with the nature of the data.
    - Non-human Research Data: Research data not related to humans.
    - Research Data; any information collected through research, defined within the ETSU Investigator's iGuide as a systematic investigation, study or experiment designed to develop or contribute to generalizable knowledge. The term encompasses basic and applied research (e.g., a published article, book, or book chapter) and product development (e.g., a diagnostic test or drug).
    - Unidentifiable Human Related Research Data: Research data related to humans but which never contained identifiers or information which could be used to identify human research subjects, as determined by the ETSU IRB.
- **Data Encryption:** Protection of data in an encoded format that requires a password, PIN, or key to activate decryption.
- **Data Storage:** Data Storage refers to a location from which data files may be accessed. Digital research data storage begins when a digital file is first named and saved on a computer.
- **FDA Research:** Any experiment that involves a test article and one or more human participants and that either is subject to requirements for prior submission to the Food and Drug Administration under Section 505(i), 507(d) or 520 (g) of the act, or is not subject to requirements for prior submission to the Food and Drug Administration under these sections of the act, but the results of which are intended to be submitted later to, or held for inspection by, the Food and Drug Administration as part of an application for a research or marketing permit.

Policy History

Effective Date: N/A

Revision Date: N/A

Procedures (see summary table below)

I. Responsibility for Digital Research Data Storage and Backup

a. All faculty, staff, and student researchers share in the responsibility for storage and backup of digital research data.

b. Student researchers should provide copies of their digital research data to their research supervisors at intervals determined with the supervisor and at the conclusion of the study or at some alternative point determined with the supervisor, pursuant to policies of the data owner. Copies of the data should always be handled in a manner that conforms to the original data storage plan as approved by the ETSU IRB.

   i. In some instances, notably clinical data within a hospital or clinic electronic health record system (EHR), it may not be permissible for student researchers to make copies of their digital research data. Students must work within the regulations of collaborating institutions and within the parameters of their protocol as approved by the ETSU IRB.

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

   i. The ETSU IRB may authorize exceptions to the 6-year rule for data not subject to other non-ETSU regulations.

d. When faculty, staff, or students depart from ETSU, they lose access to network drives, OneDrive for Business Accounts, ETSU REDCap accounts, and other network services. All departing researchers are responsible for making certain that they retain their own copy of the research data, if needed, and that an ETSU official retains a copy of the research data.

II. Appropriate Storage and Backup Locations for Digital Research Data

a. **HIPAA research data, and master lists for HIPAA research data,** that are not otherwise subject to more stringent requirements of a collaborating institution, or data use agreement, must be stored and backed up as follows:

   i. Allowable storage options:

      1. in a research project folder with access limited to authorized study staff on the HIPAA-compliant ETSU network drive (access is by request only, to the HIPAA Compliance Officer). The data are automatically backed up by ITS; or
      2. in the HIPAA compliant REDCap instance (HIPAA REDCap) with access limited to authorized study staff. Data in the HIPAA REDCap server are automatically backed up by ITS; or
      3. in the Hospital or clinic EHR System.

   ii. Required Backup Options:

      1. Backups are automatic for all allowable storage options for HIPAA research data.

   iii. Allowable Temporary and Off-Campus Storage Options:

      1. on an ETSU-owned encrypted laptop or other encrypted device. For example, researchers may need to temporarily store HIPAA research data during data collection on an ETSU-owned and encrypted device (e.g., laptop, tablet, or flash drive).
      2. HIPAA REDCap can be accessed from off campus.

   iv. Encrypted device users in data category a. must follow these guidelines:

      1. The encrypted devices may not be used by anyone outside of the approved study staff.

2. The PIN, password(s), and/or recovery key should be backed up in a secure location and a secured copy kept by the PI or by the academic unit/department.

v. Researchers who wish to use storage or backup mechanisms for HIPAA research data not outlined here must contact the ETSU HIPAA Compliance Office to discuss prior to use.

b. **Non-HIPAA Identifiable Human Subject Research Data , including but not limited to FERPA Research Data and Master Lists) for non-HIPAA Coded Human Subject Research Data** must be stored and backed up as follows:

i. Allowable Storage Options (special note: master lists must be stored separately from the coded de-identified data) In all cases, data must be stored in a research project folder with access limited to authorized study staff.

1. on an ETSU network drive. These drives are automatically backed up by ITS; or
2. in an ETSU OneDrive for Business account. ETSU OneDrive for Business is automatically backed up by Microsoft; or
3. on a secure ETSU owned desktop (see Required Backup Options immediately below); or
4. in the standard REDCap instance (REDCap). Data in the REDCap server are automatically backed up by ITS; or
5. in the Advanced Computing Facility (ACF) housed within the Joint Institute for Computational Science at the University of Tennessee/Oak Ridge National Laboratory (see Required Backup Options immediately below); or
6. in an Amazon Web Services (AWS) account set up with ETSU-ITS (see Required Backup Options immediately below).

ii. Required Backup Options (data stored in any of these locations are automatically backed up):

1. ETSU network drive; or
2. ETSU OneDrive for Business; or
3. ETSU REDCap.

iii. Allowable Temporary and Off-Campus Storage Options:

1. on any ETSU-owned encrypted device.
2. ETSU OneDrive for Business can be accessed from off campus.
3. REDCap can be accessed from off campus.
4. The ACF can be accessed from off campus.
5. AWS can be accessed from off campus.

iv. For Coded Research Data, the master list to the code must be stored securely but separately from the coded data.

v. ETSU OneDrive for Business users in data category b. must follow these guidelines:

1. ETSU OneDrive for Business accounts only; not personal OneDrive accounts.
2. Devices, other than ETSU desktops, synchronized to the OneDrive account must be encrypted.

3. Devices synchronized to the OneDrive account may not be shared beyond the research study staff.

4. Research folders should be distinct from non-research folders.

vi. Encrypted device users in data category b. must follow these guidelines:

1. The encrypted devices may not be used by anyone outside of the approved study staff.

2. The PIN, password(s), and/or recovery key should be backed up in a secure location and a secured copy kept by the PI or by the academic unit/department.

vii. Researchers who wish to use storage or backup mechanisms for non-HIPAA identifiable research data not outlined here must contact the ETSU IRB to discuss prior to use.

c. **Non-human Research Data, Unidentifiable Human-Related Research Data, and Appropriately De-Identified Human-Related Research Data (Coded or Uncoded)** must be stored and backed up as follows:

i. Allowable Storage Options:

1. Storage location is at the discretion of the researcher (backup is required). Please note that in order for de-identified coded data to be allowed under this category, the master list must be stored separately (under category b above) from the data. The master list itself does NOT fall under this category as it does not meet the definition of unidentifiable data or de-identified data.

ii. Required Backup Options (data stored in any of these locations are automatically backed up):

1. ETSU network drive; or

2. ETSU OneDrive for Business; or

3. ETSU REDCap.

iii. Allowable Temporary and Off-Campus Storage Options:

1. At the discretion of the researcher.

d. Export Controlled Information

i. If you know, or suspect that your research involves information or items that are or may be subject to Export Control Regulations, you must contact the ETSU Export Control Compliance Officer to determine the appropriate security protocols including the location for storage and backup of technology and technical data.

III. If Your Digital Research Data Exceed 1 TB.

a. If your non-HIPAA research data exceed 1 TB you should request that ITS assist you with acquisition of additional OneDrive or other storage space. Additional space on ETSU OneDrive for Business is available for approximately $70/TB/yr.

IV. If you require assistance with ETSU OneDrive for Business, please contact ITS.

a. https://www.etsu.edu/helpdesk/training/microsoft-office.php

Procedure History

Effective Date: TBD

Revision Date: TBD

Table 1. Allowable Storage, Required Backup, and Temporary and Off Campus Storage Options for Digital Research Data

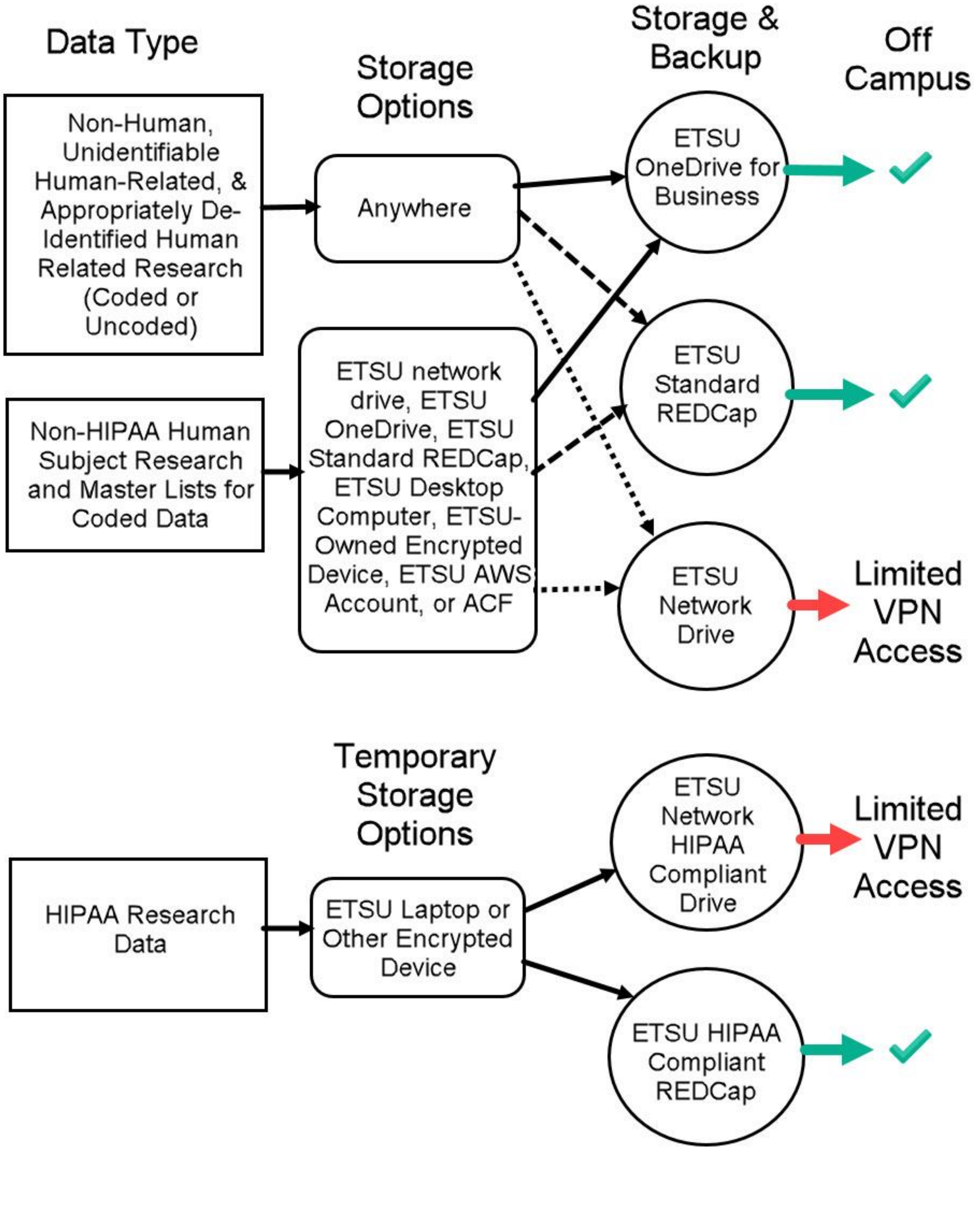
Research Data Category	**Security Risk**	**Allowable Data Storage Options**	**Required Data Backup Options**	**Allowable Temporary and Off-Campus Storage Options**
a. HIPAA Research Data, and master lists with HIPAA identifiers.	High.	• HIPAA compliant ETSU network drive[1]; or • ETSU HIPAA REDCap[2]; or • Hospital or clinic EHR System.	Backup is automatic with all allowable data storage options.	• ETSU-owned encrypted devices. • ETSU HIPAA REDCap[2] can be accessed from off campus.
b. 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[3] (automatic backup); or • ETSU OneDrive for Business (automatic backup); or • ETSU REDCap[2] (automatic backup); or • ETSU desktop; or • ETSU encrypted laptop, tablet, or external drive; or • ACF[4]; or • AWS[4].	• ETSU network drive[3]; or • ETSU OneDrive for Business; or • ETSU REDCap[2]	• ETSU-owned encrypted devices. • The following can be accessed from off campus: ○ ETSU OneDrive for Business ○ ETSU REDCap[2] ○ ACF[4] ○ AWS[4]
c. 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[3]; or • ETSU OneDrive for Business; or • ETSU REDCap[2].	At the discretion of the researcher.

Special Note: See Section III of Policy Statement 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. 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.

3. 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.
4. If you require access to ACF or AWS for advanced computing, please contact Vincent Thompson, 423.439.4492.
5. Additional information about OneDrive is found near the bottom of this page.

Figure 1: Allowable Storage, Required Backup, and Temporary and Off Campus Storage Options for Digital Research Data


Data Type
Storage Options
Storage & Backup
Off Campus
Non-Human, Unidentifiable Human-Related, & Appropriately De-Identified Human Related Research (Coded or Uncoded)
Anywhere
ETSU OneDrive for Business
✓
Non-HIPAA Human Subject Research and Master Lists for Coded Data
ETSU network drive, ETSU OneDrive, ETSU Standard REDCap, ETSU Desktop Computer, ETSU-Owned Encrypted Device, ETSU AWS Account, or ACF
ETSU Standard REDCap
✓
ETSU Network Drive
Limited VPN Access
Temporary Storage Options
HIPAA Research Data
ETSU Laptop or Other Encrypted Device
ETSU Network HIPAA Compliant Drive
Limited VPN Access
ETSU HIPAA Compliant REDCap
✓

Contacts

- For Assistance with Advanced Computing
  - Vincent Thompson, Research Computing Consultant, thompsov@etsu.edu, 423.439.4492
- For Assistance with the ETSU IRB
  - Janine Olive, Director, IRB, olivef@etsu.edu, 423.439.6504
- For Assistance with Export Control
  - Wendy Eckert, Assistant Vice President for Research and Director of Sponsored Programs, eckertw@etsu.edu, 423.439.6052
- For Assistance with HIPAA Compliance
  - HIPAA Compliance Officer – HIPAA@etsu.edu, 423.439.8533
- For Assistance with the REDCap and HIPAA REDCap Survey Instrument and Database
  - Janet Keener, Research Computing Consultant, janet@etsu.edu, 423.439.4142
- For General Assistance with regard to this policy
  - David Currie, Director, ITS-Research Computing Services currie@etsu.edu, 423.439.6457

Related Forms

The Computer Account Request and Access Form is found on the ITS Forms Page.

Scope and Applicability

✓	Governance	ETSU IRB, Office or Research and Sponsored Programs, HIPAA Compliance Officer, Export Control Compliance Officer
✓	Academic	Faculty and Staff Research and Scholarly Activity
✓	Students	Undergraduate and Graduate Student Research
	Employment	
✓	Information Technology	Information Security, Network Data Storage, Research Computing
	Health and Safety	
	Business and Finance	
	Operations and Facilities	
	Communications & Marketing	
	Advancement	