Digital Research Data Storage and Backup Policy	
Responsible Official: Vice Provost for Research and Sponsored Programs	Responsible Office: Office of Research and Sponsored Programs

Policy Purpose

The purpose of this policy is to promote 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 and to reduce the odds of data loss or inappropriate release of sensitive data through accidental means, mechanical failure, or malicious activity, and to reduce overall purchases of incidental hardware storage devices.

Policy Statement

Research Responsibilities:

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.

ETSU and its researchers share in the responsibility to secure, store, backup, 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.

Student researchers shall 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 shall always be handled in a manner that conforms to the original data storage plan as approved by the ETSU IRB.

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.

The primary investigator (PI) is responsible for storage and backup of data for a minimum of six (6) 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. The ETSU IRB may authorize exceptions to the 6-year rule for data not subject to other non-ETSU regulations.

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.

Institutional Oversight:

- 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.

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.

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.

Appropriate Storage and Backup Locations for Digital Research Data

I. 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 outlined below. 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.

Allowable storage options:

1. A research project folder on the HIPAA compliant ETSU network drive with access limited to authorized study staff (access is by request only to the HIPAA Compliance Officer; automatically backed up by ITS)
2. HIPAA compliant REDCap instance (HIPAA REDCap) with access limited to authorized study staff (automatically backed up by ITS)
3. ETSU Amazon Web Services (AWS) account within the HIPAA Perimeter (access is by request only to the Research Computing Services Department; automatically backed up by ITS)
4. Hospital or clinic EHR System

Required Backup Options:

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

Allowable Temporary and Off-Campus Storage Options:

1. HIPAA compliant ETSU network drive (can be accessed from off campus)
2. HIPAA REDCap (can be accessed from off campus)
3. ETSU Amazon Web Services (AWS) account within the HIPAA Perimeter (can be accessed from off campus)
4. 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).

Encrypted device users 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.

ETSU AWS users with HIPAA research data must follow these guidelines:

1. ETSU AWS accounts within the HIPAA Perimeter only; not personal AWS

2. Access to AWS accounts within the ETSU AWS HIPAA perimeter may only follow a request by a study PI through the PI Checklist process with ITS-Research Computing Services (ITS-RCS)

II. 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. 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.

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

1. ETSU network drive (automatically backed up by ITS)
2. ETSU OneDrive for Business account (automatically backed up by Microsoft)
3. Secure ETSU owned desktop
4. Standard REDCap instance (REDCap) (automatically backed up by ITS)
5. Advanced Computing Facility (ACF) housed within the Joint Institute for Computational Science at the University of Tennessee/Oak Ridge National Laboratory
6. ETSU AWS account set up with ETSU-ITS

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

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

Allowable Temporary and Off-Campus Storage Options:

1. 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. ETSU AWS (can be accessed from off campus)

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

ETSU OneDrive for Business users 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.

Encrypted device users 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.

ETSU AWS users must follow these guidelines:

1. ETSU AWS accounts only; not personal AWS accounts.
2. ETSU AWS Account users are requested to apply to AWS Educate for their annual compute credit; currently $100 per student and $200 per faculty.
3. Devices used to access ETSU AWS accounts should be protected by password, biometric authorization, or other lockout method.
4. Mobile devices used to access ETSU AWS accounts or other ETSU accounts should be protected by location detection software (example – Google Find My Device of Apple Find My Mac).

III. 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:

Allowable Storage Options:

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 (non-HIPAA identifiable human subject research data) must be stored separately (under category II 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.

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

1. ETSU network drive
2. ETSU OneDrive for Business
3. ETSU REDCap
4. ETSU AWS

Allowable Temporary and Off-Campus Storage Options:

At the discretion of the researcher.

IV. Export Controlled Information

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.

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

- 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
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 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)
- Tennessee Data Disposal Regulation Tenn. Code Ann. § 39-14-150
- Tennessee Financial Records Privacy Act Tenn. Code Ann. § 45-10-*

Definitions

Data Backup	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	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 or as determined by the ETSU IRB or as determined by the ETSU HIPPA Compliance Office. • 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	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: Approved by University Council: 6/11/2018

Procedures

1. If non-HIPAA research data exceed 1 TB, request that ITS assist with acquisition of additional OneDrive or other storage space. Additional space on ETSU OneDrive for Business is available for approximately $70/TB/yr.
2.

For assistance with:	Contact:
• ETSU OneDrive for Business	ITS
• Advanced computing	Research Computing Services
• IRB policy	IRB Office
• Export control	Office of Research and Sponsored Programs
• HIPAA compliance	HIPAA Compliance Officer
• REDCap and HIPAA REDCap survey instrument and database	Research Computing Services
• General assistance with this policy	Director, ITS-Research Computing Services

Procedure History

Effective Date: Approved by University Council: 6/11/2018

Related Forms

The Computer Account Request and Access Form is found on the ITS Forms Page.
Data Storage and Backup Chart
Data Storage and Backup Flow Cart

Scope and Applicability

✓	Governance	
✓	Academic	
✓	Students	
	Employment	
✓	Information Technology	
	Health and Safety	
	Business and Finance	
	Operations and Facilities	
	Communications & Marketing	
	Advancement	