ADMINISTRATIVE POLICY

Subject: **Information Security**	Page: 1 of 4	Policy # Version: **2.0**
Title: **FSM Data Storage Policy**	Revision of: **Version 1.0**	Effective Date: **5/1/2019**
		Removal Date:

I. PURPOSE

This policy defines the requirements and procedures for securely storing Feinberg School of Medicine (FSM) research, educational, and administrative data. It outlines approved data storage platforms based on the sensitivity of the data and compliance with regulatory requirements, including the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Family Educational Rights and Privacy Act (FERPA), and the Illinois Personal Information Protection Act (815 ILCS 530/1), ensuring proper data backup, restoration, and secure access to sensitive information.

II. POLICY STATEMENT

FSM is committed to the secure storage of research, educational, and administrative data. All data must be stored on approved platforms, in compliance with Northwestern University (NU) policies, legal regulations, and relevant contractual obligations.

Third-party services must be FSM-approved and used under established contracts signed by authorized personnel listed in the NU Authorized Signatory List. Faculty and staff who are not authorized signatories may not enter into or sign agreements. The use of personal or non-NU contracted storage services is strictly prohibited to ensure compliance with security and legal standards.

This policy supplements, and does not supersede, NU policies governing research, the Institutional Review Board (IRB), and agreements with external vendors and research collaborators.

III. PERSONS AFFECTED

All FSM faculty, staff, students, residents, fellows, as well as any individuals with access to FSM data, including those involved in studies where Northwestern Memorial HealthCare (NMHC) is identified as a site of research.

IV. PROCEDURE STATEMENT

Data Classification

All data storage, whether internal or external, must adhere to NU Data Classification Policy and the storage options outlined in this procedure to ensure appropriate security and handling based on data sensitivity.

Protected Health Information (PHI) refers to any health-related information that can identify an individual and is protected under HIPAA. This includes data such as medical records, billing information, and health conditions tied to personal identifiers. All PHI must be stored and handled in compliance with HIPAA regulations and any applicable agreements governing its secure use, sharing, and protection, including those established for research.

Personally Identifiable Information (PII) refers to any information that can be used to identify an individual, whether alone or in combination with other data. PII includes identifiers such as names, Social Security numbers, email addresses, phone numbers, and financial details. While PII is not protected under HIPAA unless it pertains to health information, it must be handled in accordance with applicable privacy laws and institutional policies. All PII must be stored securely and in compliance with applicable agreements, such as Data Use Agreements (DUAs).

Approved Storage Platforms

Service	Level 1 (Public)	Level 2 (Internal)	Level 3 (PII)	Level 3 (PHI)
FSM-managed devices including desktop, laptop, server, virtual machine, and removable storage	Yes	Yes	Yes	Yes
FSMResFiles	Yes	Yes	Yes	Yes
Microsoft OneDrive	Yes	Yes	Yes	Yes
Microsoft SharePoint	Yes	Yes	Contingent	Contingent
Microsoft Azure*	Yes	Contingent	Contingent	Contingent
Research Data Storage Services (RDSS)	Yes	Contingent	Contingent	No
Amazon Web Services (AWS)*	Yes	Contingent	Contingent	No
Google Cloud Platform (GCP)*	Yes	Contingent	Contingent	No
Quest Storage	Yes	Contingent	Contingent	No
Personally-owned devices	Yes	Contingent	No	No

*GCP is not approved for general use and will only be considered for specific use cases, making Azure and AWS the recommended options for most research and administrative storage needs due to their integration with existing security frameworks and institutional support.

Additional Notes

- FSM-managed devices: External storage must be purchased and configured by Feinberg IT. Physical servers must be in the NU data center and managed by FSM IT. Determined on a case-by-case basis, physical servers with attached laboratory equipment must remain secured in the laboratory.
- Contingent: Platforms require an IT assessment, and safeguards must comply with NU and FSM policies, as well as any applicable agreements, to ensure the security, integrity, and confidentiality of the data.

Prohibited Storage Platforms

Personally-contracted cloud storage services (e.g., Box, Dropbox, iCloud) and personal removable storage devices are strictly prohibited for storing institutional or sensitive data to ensure compliance with security and legal standards. Only FSM-approved platforms, including those identified through Sponsored Research contracts, may be used for storing, transferring, or accessing data.

Data Handling

Security requirements must align with the NU Endpoint Security Standard, FSM Authorization and Access Control Policy, and the recommendations of the NU Cloud Community of Practice for storing, transferring, and accessing data.

Data Backup

All backup activities must comply with the FSM Data Backup Policy.

Data Retention

All data retention activities must comply with the NU Research Data: Ownership, Retention, and Access, as well as any specific data retention requirements outlined in applicable agreements or funding agency policies.

V. EXCEPTIONS

Any exceptions to this Policy must be documented in writing and approved by the FSM IT Steering Committee.

VI. POLICY UPDATE SCHEDULE

This policy will be reviewed one year after its initial implementation and subsequently every three years.

VII. REVISION HISTORY

01/14/2025 – General updates to align with new NU and FSM policies.
05/01/2019 – New policy effective.

VIII. RELEVANT REFERENCES

NU Appropriate Use of Electronic Resources
https://www.it.northwestern.edu/about/policies/appropriate-use-of-electronic-resources.html

FSM Information Security and Access Policy
https://www.feinberg.northwestern.edu/it/docs/information_security_and_access_v3.pdf

NU Data Classification Policy
https://policies.northwestern.edu/docs/data-classification-policy.pdf

NU Endpoint Security Standard
https://www.it.northwestern.edu/about/policies/endpoint-security.html

FSM Authorization & Access Control Policy
https://www.feinberg.northwestern.edu/it/docs/access-control-policy-02.28.18.pdf

NU Cloud Community of Practice
https://www.cloud.northwestern.edu/recommendations/

FSM Data Backup Policy
https://www.feinberg.northwestern.edu/it/docs/data-backup-policy-02.28.18.pdf

NU Research Data: Ownership, Retention, and Access
https://researchintegrity.northwestern.edu/resources/research-data-policy.pdf

FSMResFiles Research Data Storage
https://www.feinberg.northwestern.edu/it/services/server-storage-and-data/research-data-storage.html

NU Research Data Storage Service (RDSS)
https://services.northwestern.edu/TDClient/30/Portal/Requests/ServiceDet?ID=96

Health Insurance Portability and Accountability Act (HIPAA)
http://www.hhs.gov/hipaa/for-professionals/index.html

Health Information Technology for Economic and Clinical Health (HITECH)
http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

Family Educational Rights and Privacy Act (FERPA)
https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Illinois Personal Information Protection Act (815 ILCS 530/1)
http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67

XI. CONTACT INFORMATION

Please address all questions and requests for IT resources (e.g., storage and storage estimates, backup storage, archiving storage, granting access to data) to fsmhelp@northwestern.edu.

Please address all questions, request for clarification, and all other forms of assistance regarding this policy to fsmit-policy@northwestern.edu.