Subject: **Information Security**	Page **1 of 4**	Policy # **Version: 1.0**
Title: **FSM Data Storage Policy**	Revision of: **Feinberg Guidelines for File Storage**	Effective Date: **05/01/2019**
		Removal Date:

I. PURPOSE

This policy and procedure establishes the requirements for storing FSM research, administrative and educational data. These requirements include approved data storage platforms based on the sensitivity of the data, the ability to execute reliable data backup and recovery procedures, and manageability and configurability of data access control.

The Health Insurance Portability and Accountability Act (HIPAA), The Health Information Technology for Economic and Clinical Health (HITECH) Act, Family Educational Rights and Privacy Act (FERPA), and Illinois Personal Information Protection Act (815 ILCS 530/1) were essential in defining these Policy requirements. Example applicable HIPAA Security Rule requirements include data backup, 164.308(a)(7)(ii)(A); data restoration, 164.308(a)(7)(ii)(B); and data access, 164.312(a)(1).

II. PERSONS AFFECTED:

All NU staff, faculty and students that retain information that supports FSM education, research or administrative activities.

III. POLICY STATEMENT

FSM research and administrative data must be stored consistent with the Data Storage Options defined in the procedure. These data storage options include those provided by and approved by NU or FSM only for the purposes indicated.

Some data storage options are available from external service providers under contracts established by NU. Use of these services must occur within the environment established by NU contracts and as defined in the Procedure. Individually or personally contracted services is not permitted (e.g., NU Box permitted to the extent the Procedure allows, personal Box accounts not permitted).

Use of data storage options is based on the Standards for Data Classification defined in the NU Data Access Policy[2]. Access to data is allowed as defined in the FSM Authorization & Access Control Policy[3]. Data backup procedures are defined in the FSM Data Backup Policy[4]. Pertinent information is included in the FSM Cloud Services Policy[15] and the Relevant Resources section of this policy.

This policy does not supersede any NU policies and is supplemental to NU policies governing NU Research and the NU IRB and execution of contracts and agreements with other external vendors and collaborators.

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

IV. PROCEDURE STATEMENT

Use of data storage options in this procedure is based on the **Standards for Data Classification**[2] defined in the **Standards for Data Classification**[2].

Data Storage Options as indicated in the following tables	**Public Information**[2]	**Internal Information**[2]	**Legally/Contractually Restricted Information**[2]
Examples	Conference poster presentations	De-identified data per HHS guidelines	ePHI (patient medical records, recruitment data from medical record systems or equivalent)
	Published research manuscripts	Sponsor and grant contracts	PII (study participant data under consent, personnel records, social security numbers)
	NIH ClinicalTrails.gov registry	Pre-publication and interim study reports	FERPA (student records)
		Data security plans	Illinois Personal Information Protection Act (personal financial records)

Y = Data of the specified classification is permitted to use the data storage option.
N = Data of the specified classification is not permitted to use the data storage option.

FSM Managed Services	**Public Information**[2]	**Internal Information**[2]	**Legally/Contractually Restricted Information**[2]
Desktop/laptop Encryption required[1]	Y	Y	Y Server-storage preferred
External detachable storage e.g., any USB attachable storage devices Encryption required[1]	Y	Y	Y
Server (Windows, Linux)	Y	Y	Y

Network Attached Storage (NAS) is not permitted. Physical servers must be located 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.

IV. PROCEDURE STATEMENT *continued*

Personally-Owned Devices	**Public Information[2]**	**Internal Information[2]**	**Legally/Contractually Restricted Information[2]**
Any type of personally-owned device capable of storing data	Y	N	N

NU Contracted Cloud Services	**Public Information[2]**	**Internal Information[2]**	**Legally/Contractually Restricted Information[2]**
Amazon Web Services[9, 15]	Y	Y	Y
Microsoft Online Services[15] Azure[9] O365 / OneDrive[10] Sharepoint[11] Skype[12]	Y	Y	Y
NU Box[7]	Y	Y	N
NU Google @u.northwestern.edu	Y	N	N
Google Drive	Y	N	N
Google Cloud	Y	N	N
IBM Bluemix	Y	N	N
Apple iCloud	Y	N	N
Dropbox	Y	N	N

IV. PROCEDURE STATEMENT *continued*

NU Services	Public Information[2]	Internal Information[2]	Legally/Contractually Restricted Information[2]
FSM RESFILES[6] (NU Research Data Storage Services)	Y	Y	Y
Quest[8]	Y	Y	N
Skype[12]	Y	Y	Y
WebEx[13]	Y	Y	N
BlueJeans[14]	Y	Y	N

V. ROLES AND RESPONSIBILITIES

FSM IT Security will oversee the data storage policy and provide oversight, direction and reporting regarding compliance.

Custodians, owners and users of data will be responsible to ongoing compliance with this Policy.

VI. POLICY UPDATE SCHEDULE:

Policy review to occur one year after initial implementation and every three years thereafter.

VII. REVISION HISTORY:

05/01/19 – New policy effective.

VIII. RELEVANT REFERENCES:

[1]FSM General Information Security Policy:
https://www.feinberg.northwestern.edu/it/docs/General-Security-Policy-092216-V2-1.pdf

[2]NU Data Access Policy:
https://www.it.northwestern.edu/policies/dataaccess.html

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

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

[5]File Sharing at Northwestern:
https://www.it.northwestern.edu/file-sharing/overview.html#service

[6]NU Research Data Storage:
https://www.it.northwestern.edu/research/user-services/storage/research-data.html

[7]NU Box
https://www.it.northwestern.edu/file-sharing/box.html

[8]NU Quest High Performance Computing Cluster
https://www.it.northwestern.edu/research/user-services/quest/

[9]NU Cloud Initiatives (AWS, Azure)
https://www.cloud.northwestern.edu/

[10]NU OneDrive for Business
https://www.it.northwestern.edu/file-sharing/onedrive.html

[11]NU Sharepoint
https://www.it.northwestern.edu/collaborate/sharepoint/index.html

[12]Skype for Business/Lync Overview
https://www.it.northwestern.edu/collaborate/lync/index.html

[13]WebEx at Northwestern
https://www.it.northwestern.edu/conferencing/webex/index.html

[14]BlueJeans Conferencing Service
https://www.it.northwestern.edu/conferencing/bluejeans/index.html

[15]FSM Cloud Services Policy
https://www.feinberg.northwestern.edu/it/docs/Cloud_Security_Policy_V1_1.pdf

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