ADMINISTRATIVE POLICY

Subject: **Information Security**	Page: 1 of 4	Policy # Version: **3.0**
Title: **FSM Information Security and Access**	Revision of: **Version 2.1** **9/22/2016**	Effective Date: **6/14/2024**
		Removal Date:

I. PURPOSE

The Feinberg School of Medicine (FSM) is committed to the highest standards of protecting electronic patient, research, and other sensitive information in accordance with our legal and ethical responsibilities. This policy aims to prevent unauthorized disclosure, modification, and destruction of data, which can have serious consequences for research integrity, patients, and the reputation of Northwestern University (NU) and its partners.

II. POLICY STATEMENT

FSM requires that protected data used for research, education, or administrative functions meet, at a minimum, the standards outlined by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Additionally, any activity subject to other regulations, grants, agreements, or contracts must comply with the specific security requirements of those provisions as well.

III. PERSONS AFFECTED

All FSM faculty (including adjunct, emeritus, and visiting), staff, students, residents, fellows, and individuals with access to FSM data, systems, or facilities.

IV. PROCEDURE STATEMENT

Overview

This policy augments existing FSM and NU information security policies, procedures, and guidelines. Where this FSM policy is more restrictive than NU policies, procedures, and guidelines, this FSM policy applies. Personal devices accessing NU data or electronic resources must comply with all relevant NU and FSM policies.

Data Protection

- All portable devices and desktop computers, including laptops, tablets, USBs, and smartphones must be encrypted.
- Electronic transmission of data, including emails, web connections, and file transfers, must be encrypted.
- De-identification of data, whether by NU employees handling Northwestern Memorial HealthCare (NMHC) data, medical students working with patient data, non-human subjects research, or IRB-approved research studies, must be done in accordance with relevant policies and guidelines, including protocols, consent forms, and applicable policies from affiliate organizations, such as NMHC's Privacy and Confidentiality Policy.

Data Storage

- Data must be stored on storage solutions that are approved by NU and FSM.
- Use of Network Attached Storage (NAS), servers located outside the NU data center without a justified operational requirement (e.g., attached laboratory equipment), or workstations functioning as servers (e.g., hosting web services) is prohibited.
- Offsite storage services are permitted only with approval from the FSM Dean's Office and relevant business units, such as Sponsored Research (SR) or Office of General Counsel (OGC), and must comply with grant or contract requirements.
- Regular data backups, aligned with grant or contract stipulations, are required and must be stored on approved secure storage.

Access Control and Security

- Access to electronic and physical information is granted only to authorized individuals, with additional IRB approval required when applicable.
- Access to electronic information requires the use of complex passwords, as defined by NU policy, including PINs for smartphones, and prohibits the sharing of credentials, including API tokens.
- Privileged account holders must not abuse their access on FSM-owned devices and must refrain from making unauthorized changes to security settings, creating local accounts, installing unapproved software, or modifying devices or systems that may compromise security.
- Only employed faculty, staff, students, approved contractors, and vendors who have executed a formal agreement with NU are permitted to perform tasks requiring special access, such as software development, application support, and system administration, within their designated roles and with authorization from the FSM Dean's Office. See additional guidance on Special Access under Relevant References.

Monitoring and Reporting

- Any suspicion or confirmation of a data breach, including unauthorized data access, equipment theft, or removal of documents and storage devices, must be reported immediately to FSM IT.
- Audit logs must be enabled across networks, endpoint devices, and applications to ensure traceability of access to protected information.
- Regular audits, risk analysis, and vulnerability assessments are conducted under the direction of the FSM Dean's Office.

Data Handling and Vendor Management

- All research projects seeking NU Institutional Review Board (IRB) approval, including those using an External IRB, must have a Data Security Plan (DSP).
- All contracts and agreements must follow FSM's Contract Review Process guidelines.
- Use of public email systems, such as Gmail, are not approved for any FSM purposes.
- Use of unapproved generative AI tools or cloud-based services to process or store institutional data is prohibited.

Training and Awareness

- Annual security awareness and privacy training is mandatory for those listed on the Authorized Personnel List (APL) of an IRB-approved protocol.

Ownership

- NU retains ownership of institutional data and equipment, including email, unless otherwise stipulated in an agreement or explicitly designated as an exception.

V. EXCEPTIONS

Exceptions to this policy require approval by the FSM Dean's Office. Exceptions may be revoked if the capabilities allowed through the exception are used inappropriately. Please send requests to fsmit-policy@northwestern.edu.

VI. COMPLIANCE AND ENFORCEMENT

Changes to the technology environment affecting information security will be recorded and approved in the FSM IT change management systems. Failure to comply with these policies will lead to sanctions, up to and including administrative suspension of NetID, loss of faculty appointment, department or unit financial penalties, or dismissal from NU.

VII. POLICY UPDATE SCHEDULE

No less than every five (5) years, but more frequent updates may be conducted as required.

VIII. REVISION HISTORY

06/14/2024 – General updates to align with new NU and FSM policies.
04/15/2016 – Replaces existing policy.
09/22/2016 – Clarification of procedure statement #22.

IX. RELEVANT REFERENCES

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

National Institute of Standards and Technology (NIST)
http://csrc.nist.gov/

Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

FSM Information Security Policies
https://www.feinberg.northwestern.edu/it/policies/information-security/index.html

FSM Contract Review Process
https://www.feinberg.northwestern.edu/finance/financial-management/contracts-events.html

Northwestern Policies, Standards, and Guidelines
https://www.it.northwestern.edu/about/policies/

Secure IT at Northwestern
http://www.it.northwestern.edu/security/

Service Provider Security Assessments
http://www.it.northwestern.edu/about/departments/itms/cpo/assessment.html

Northwestern Guidance on the Use of Generative AI
https://www.it.northwestern.edu/about/policies/guidance-on-the-use-of-generative-ai.html

Northwestern Memorial HealthCare
https://irb.northwestern.edu/docs/research-privacy-and-confidentiality-policy.pdf

Additional Guidance on Special Access

Roles with special access (as job duties required):

- Faculty (including but not limited to): Associate Dean, Associate Professor, Assistant Professor, Chairperson, Dean, Librarian, Professor, Research Assistant Professor, Research Associate Professor, Research Professor
- Staff, approved contractors, and vendors
- Postdoc / Research Associate: Clinical Research Associate, NRSA Postdoc Fellow, Post Doc - Dept of Education, Postdoctoral Scholar, Research Associate, Research Associate Senior, Sr Clinical Research Associate

Roles with limited or no special access include, but not limited to:

- Former Affiliates: Former employees and students
- Temporary and Adjunct Roles: Temporary staff (students and non-students), adjunct faculty, and visiting scholars (e.g., Visiting Professors, Adjunct Instructors)
- Health System Clinicians
- Emeritus Faculty: Retired faculty members with emeritus status
- Contributed Services Faculty: Clinical faculty providing services on a part-time or contributory basis
- Graduate Students and Residents / Fellows: Graduate students, teaching assistants, research assistants, and medical residents/fellows
- Other affiliations: Staff from affiliated institutions or administrative roles (e.g., NMFF Department Administrators, NMG Department Assistants, Manne Administration / Research Staff)

X. CONTACT INFORMATION

Please address all questions, report incidents, or requests for exceptions 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.