ADMINISTRATIVE POLICY

Subject: **Information Security**	Page: **1 of 5**	Policy # Version: **2.0**
Title: **Data Security Plan Requirements for FSM Research**	Revision of: **Version 1.1** **4/21/2017**	Effective Date: **3/26/2024**
		Removal Date:

I. PURPOSE

This policy safeguards the data used for all human research projects involving research studies at the Feinberg School of Medicine (FSM) and those outside FSM that indicate Northwestern Memorial HealthCare (NMHC) as a research site. It applies to every stage of data handling – including collection, storage, transmission, analysis, and reporting – regardless of whether the projects are non-human subjects research, exempt, expedited, or subject to full board review.

This policy applies to new research applications, re-applications, and studies at the continuing renewal stage following this policy's effective date. While it is aligned with the Northwestern University Institutional Review Board (NU IRB) Policy, this policy independently outlines the requirements for data safeguarding within the scope of IRB-submitted research at FSM and with NMHC.

II. POLICY STATEMENT

All research projects submitted to the NU IRB, whether human or non-human subject research, must submit a Data Security Plan (DSP) and obtain approval. This policy applies to studies relying on an External IRB. The DSP must align with the guidelines outlined in this policy and any stipulations outlined in the individual research grant or contract. A DSP is mandatory for all projects with an FSM Principal Investigator (PI) or Co-Investigator (Co-I), as well as for studies that involve NMHC as a site of research, to ensure the proper protection and management of research data. This policy does not apply to animal-related research projects or matters overseen by the Institutional Animal Care and Use Committee (IACUC).

The PI is responsible for ensuring that the DSP is thorough and suitable for the research project and for maintaining its accuracy throughout the project. Any DSPs can be selected for internal audits by NU or external third-party organizations, further underscoring the PI's need to ensure proper and compliant use of the DSP throughout the research project.

III. PERSONS AFFECTED

All FSM faculty, staff, students and trainees engaging in research and any personnel with studies involving NMHC as a site of research.

IV. DATA SECURITY PLAN REQUIREMENTS

Authoring Data Security Plans

The PI is required to create a DSP by addressing each of the seven components defined in this policy. The PI must sign and document the DSP, which will be stored in the official study files and uploaded to the Research Supplemental System (RSS), a part of the eIRB workflow.

Data Security Plan Template

The required template for the DSP is accessed and completed during the protocol submission in the RSS section of eIRB. The template ensures that all necessary sections are completed per policy guidelines.

Human Research Determination

Identify whether a study involves human research. Compliance with the human research determination process must be achieved in one of two ways:

- Submitting the completed HRP-503 form through the DSP process, or
- Directly submitting the completed form to the IRB for a formal review and determination using their standard procedure.

Data Custodian

The Data Custodian is a designated individual accountable for the data's lifecycle during the research project. The Data Custodian oversees the DSP's creation, compliance, and updates, as well as the ongoing security of the research data.

The Data Custodian is typically the PI, but the secondary individual, such as a Co-I or research team member, should be identified as a backup. Their roles must be clearly identified in the protocol.

Data Classification

Identify the sensitivity level of the data gathered as part of the research using the Northwestern University Data Classification Policy. Consider any information mandated by law when classifying the data to be safeguarded (e.g., under HIPAA, FERPA, Illinois Personal Information Protection Act) or any data whose unauthorized disclosure might lead to legal or financial implications for the University or clinical partners. The sensitivity classification of the data must align with these considerations and legal requirements.

Data Flow & Transmission

Outline how data will be collected, shared, and transmitted securely from the source to every processing location and platform.

Data Storage

Identify the storage locations for your data, ensuring compliance with the Feinberg Data Storage Policy.

Data Access & Sharing

Identify who will access the data, including third-party vendors, external institutions, government agencies, or corporate entities. Ensure that access aligns with NU Appropriate Use of Electronic Resources Policy, Feinberg Information Security & Access Policy, NU IRB Study Team Requirements, and applicable NU Sponsored Research Agreements.

Data Backup & Recovery

Identify the data storage for backup and recovery of non-reproducible data and custom programming for the research project in the event of equipment failure, physical facilities impairment, or natural disasters.

Data Retention

Upon completing the research project, describe how the data will be moved from the active storage location to a secure, long-term storage location. Mention the length of data retention as per the grant, contract, or NU Retention of University Records policy.

V. EXCEPTIONS

Exceptions to this Policy may be considered given appropriate research and business justification. Requests which will unduly raise the risk of inadvertently exposing protected health information and personally identifiable information will not be approved. Please send requests to fsmit-policy@northwestern.edu.

VI. COMPLIANCE AND ENFORCEMENT

Research applicants must ensure compliance with underlying Feinberg School of Medicine Policies & Procedures, overarching Northwestern University Policies & Procedures, and human subject protection regulations which include: Protection of Human Subjects (45 CFR 46, 21 CFR 50); Institutional Review Boards (21 CFR 56); HIPAA Privacy (45 CFR 160, 45 CFR 164 Subparts A and E); HIPAA Security (45 CFR 160, 45 CFR 164 Subparts A and C); HITECH Act of 2009; The Family Educational Rights and Privacy Act of 1974 (FERPA); and relevant application State and local regulations.

Failure to comply with these policies will lead to sanctions, up to and including administrative suspension of activities, loss of faculty appointment, department or unit financial penalties, or dismissal from the University.

VII. DEFINITIONS

eIRB (electronic Institutional Review Board system): Portal for electronic submission of research proposals to the IRB

HIPAA: Health Insurance and Portability and Accountability Act of 1996 and the privacy regulations under that Act

Institutional Review Board (IRB): A federally mandated body that reviews and approves research in accordance with federal regulations including, but not limited to DHHS regulations at 45 CFR 46 and its subparts, as well as FDA requirements at 21 CFR 50 and 21 CFR 56. When research involving products regulated by the FDA is funded, supported or conducted by FDA and/or DHHS, both the DHHS and FDA regulations apply. The IRBs have a central role in ensuring that human subject research is planned and conducted in an ethical manner, and in compliance with federal and state regulations.

Principal Investigator (PI): The individual with primary responsibility for the design and conduct of a research project. The PI is also responsible for ensuring that all individuals who work under the supervision of the PI and participate in the conduct of the research have adequate education in order to discharge their duties in a manner that is consistent with the federal regulations for protection of human subjects as well as with this policy and with the specific requirements of the NU IRB.

Protected Health Information (PHI): Any patient or individually identifiable health information.

Personally Identifiable Information (PII): Any data collected directly from a respondent or research participant, such as through surveys or interviews.

Research: As defined by the Department of Health and Human Services (DHHS), a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. DHHS regulations further define a human subject as a living individual about whom an investigator (whether professional or student) conducting research obtains either: (a) data through intervention or interaction with the individual or (b) identifiable private information.

Sponsor: For the purposes of this policy, a sponsor is limited to a person or entity that provides funding to cover the expenses to conduct the research study. A study sponsor is usually the entity that developed the drug or device being used in a clinical investigation, but could also be any person or entity that serves as funding source for the research study. Therefore a sponsor can be external to Northwestern (e.g. drug or device company, an NIH Institute...etc) or internal to Northwestern (such as an NU Department, NMF grant...etc).

VIII. POLICY UPDATE SCHEDULE

Policy review to occur no less than annually.

IX. REVISION HISTORY

03/26/2024 – New DSP requirements for FSM research.
04/21/2016 – General clarifications and updates to coincide with template version 1.4.
09/01/2014 – New policy effective.

X. RELEVANT REFERENCES

Data Security Plans Frequently Asked Questions (FAQ)
http://www.feinberg.northwestern.edu/it/policies/information-security/data-security-plans.html

Feinberg Data Storage Policy
https://www.feinberg.northwestern.edu/it/docs/feinberg_data_storage_policy.pdf

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

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

Northwestern University Institutional Review Board (IRB)
https://irb.northwestern.edu/submitting-to-the-irb/

Northwestern University Retention of University Records
https://policies.northwestern.edu/docs/Retention_of_University_Records_030410.pdf

XI. CONTACT INFORMATION

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

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