I. **PURPOSE:**

Maintaining the privacy, security and integrity of data about our research participants, students, and staff is both an ethical and legal responsibility. As a result of the nature of clinical care and biomedical research, staff at the Feinberg School of Medicine (FSM) are much more likely to collect, use, manage and be exposed to Personal Health Information (PHI) and Personally Identifiable Information (PII) than are staff at most other schools within Northwestern University (NU). In order to address this need FSM has developed additional policies regarding the appropriate use of electronic resources that work in concert with NU-wide policies.

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.

II. **POLICY STATEMENT:**

1. NU faculty, staff, students, and trainees are required to comply with NU policies on appropriate use of electronic resources and the responsible conduct of research.

2. FSM faculty, staff, students, and trainees are also required to comply with FSM-specific policies. In cases where the FSM policy is more restrictive or more defined than the broader NU policy, FSM personnel are required to follow FSM policy.

3. Unless otherwise contractually specified, all research and operational data are the property of NU.

4. Unless specifically stated otherwise in NU or FSM policy, the guidelines of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act should be considered the minimum standard for handling PHI or PII.

5. Faculty members and managers are responsible for ensuring that their employees and students are conducting all work in full accordance with NU and FSM Information Security and Access Policies. FSM staff, students and trainees are required to work with their managers to ensure compliance with these policies.

6. Additional restrictions govern PHI and PII that are shared with collaborators and organizations outside of FSM. FSM faculty, staff, students, and trainees are also required know and to comply with such policies.

7. All members of the NU and FSM community are required to report violations of NU or FSM IT security policy. Violations can be reported at: FSMIT-policy@northwestern.edu. Other reporting options are detailed at: www.it.northwestern.edu/policies/reporting.html.

8. Any actual or suspected data breach (including unauthorized access to or compromise of data, theft or removal of equipment, papers, storage media, etc.) must be reported immediately to: FSMIT-policy@northwestern.edu

9. Any PHI or PII that is collected, processed, transmitted or stored on University Electronic Resources or supported devices must adhere to University encryption and authentication standards. Personal devices (including smartphones, tablets and home computers) that connect to FSM resources are required to comply with these policies.

10. Any researcher or project that chooses to store PHI, PII or research data on devices or servers other than those centrally managed by FSMIT or NUIT staff is responsible for documenting data
11. Ongoing risk assessments and audits will be conducted to verify compliance with this policy.

**FSM IT Security DOs and DON’Ts**

This represents a short, easily remembered, list of actions that FSM staff and researchers should do to minimize the most common Data Security Risks

- PHI, PII, and research data must be stored and backed up in a secure environment (both physical and digital security).
- “If it moves, encrypt it.” Specifically:
  - Any mobile or carry-able device or storage media that contains PHI, or PII must be encrypted (including smartphones, USB or removable drives, memory cards, portable computers, tablet computers, tapes, removable or portable disk drives, iPads, desktop computers, etc.).
  - Any electronic transmission that contains PHI, or PII must be encrypted (e.g. emails, web connections, transmitted files, etc.).
  - Any desktop, workstation, blade server or similar computing device that holds PHI or PII and is not operated within an FSM-approved datacenter or like facility must be encrypted using a University-approved solution.
  - Any device containing PHI, PII, or research data should be password protected in accordance with the NU password policy. With the exception of phones, which may use a 4-digit pin, strong passwords must be used.
  - No shared accounts or passwords for access to PHI or PII.

III. **PERSONS AFFECTED:**
All FSM faculty, staff, students and trainees.

IV. **DEFINITIONS:**

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

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

**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.

V. **POLICY UPDATE SCHEDULE:**
No less than every five (5) years, but more frequent updates may be conducted as required.

VI. **RELEVANT REFERENCES:**
NUIIT Policies, Guidelines, and Practices: [http://www.it.northwestern.edu/policies/](http://www.it.northwestern.edu/policies/)