General Security Policy

- 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.
- Feinberg faculty, staff, students, and trainees are also required to comply with Feinberg-specific policies. In cases where the Feinberg policy is more restrictive or more defined than the broader NU policy, Feinberg personnel are required to follow Feinberg policy.
- Unless otherwise contractually specified, all research and operational data are the property of NU.
- Unless specifically stated otherwise in NU or Feinberg 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.
- Faculty members and managers are responsible for ensuring that their employees and students are conducting all work in full accordance with NU and Feinberg Information Security and Access Policies. Feinberg staff, students and trainees are required to work with their managers to ensure compliance with these policies.
- Additional restrictions govern PHI and PII that are shared with collaborators and organizations outside of Feinberg. Feinberg faculty, staff, students, and trainees are also required know and to comply with such policies.
- All members of the NU and Feinberg community are required to report violations of NU or Feinberg 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.
- 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
- 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 Feinberg resources are required to comply with these policies.
- Any researcher or project that chooses to store PHI, PII or research data on devices or servers other than those centrally managed by Feinberg IT or NUIT staff is responsible for documenting data security policies, procedures and activity (including audit logging) annually to the Feinberg Chief Information Security Officer.
- Ongoing risk assessments and audits will be conducted to verify compliance with this policy.

Feinberg IT Security DOs and DON'Ts

This represents a short, easily remembered, list of actions that Feinberg 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 Feinberg-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 four-digit pin, strong passwords must be used.
- No shared accounts or passwords for access to PHI or PII.