Northwestern Medicine®
Feinberg School of Medicine

Feinberg School of Medicine and Department of Urology
Information Technology and Security Policies

The Feinberg School of Medicine (FSM) and the Department of Urology are committed to the highest standards of protecting electronic patient, research, and other sensitive information in accordance with our legal and ethical responsibilities. This information needs to be protected in all aspects of our research and other activities, including unauthorized disclosure, modification and destruction of data.

Electronic Transmission of Data and Device Encryption Policy

- Email messages and attachments are required to be sent encrypted when containing PHI or PII. Encryption may occur automatically, manually or placed into quarantine. Methods of encryption can be found **here.**
- The use of public email systems (e.g., Gmail) are not approved for any Feinberg purposes.
- All laptops, handheld devices and portable storage devices of all types must be encrypted. Feinberg IT will encrypt these devices prior to delivery to the end user.
- Mobile devices like iPhones, iPads, and Android and Windows phones are compliant if encrypted. This happens automatically with most devices when a pin is used.

Data Storage

- PHI and Proprietary Business Information should never be saved to mobile storage devices, including laptops.
- PHI must be stored on **FSMfiles** or SharePoint.
- Cloud storage (e.g., Microsoft OneDrive, Google Drive), and Box.com is not allowed.
- The **Data Security Plans for Information Used in Clinical Research policy and procedure** defines the requirements for handing personal or health-related identifiable information within the context of clinical research.

IT Hardware and Software Purchasing

- Any IT purchase, whether intended for NU or NM funds, should be discussed with Urology department administrator to determine procurement process and funding source. Hardware or software not purchased through FSM or NM IT will not be reimbursed.
- All devices with a hard-drive must be purchased, onboarded, and deployed by **Feinberg IT Procurement**. These devices include laptops, desktops, tablets, flash drives, and external hard drives. If your desired item is not obtainable through Feinberg IT or listed on their site, consult Feinberg IT at **fsmhelp@northwestern.edu**.
- University-owned and licensed software can only be installed on university-owned computers (with the exception of those vendors' products that are licensed under a home use policy); learn more via the following links: **Microsoft Software** and **Adobe Software.**

Northwestern Medicine®
Feinberg School of Medicine

Research Use of Electronic Medical Data

- Manual chart abstraction for research purposes is prohibited.
- Data recorded in Northwestern Medicine electronic medical records systems (e.g., EPIC, Cerner) for clinical care and desired to be used for research must be obtained from the **Northwestern Medicine Enterprise Data Warehouse** (EDW).
- All NMEDW data requests should be limited to data that is required to conduct the study consistent with the approved IRB protocol or with policies and laws governing preparatory-to-research requests.
- A determination if the NMEDW is insufficient to meet research needs will be derived from a collaboration of the NMHC Data Steward, the principal investigator, and the Chief Information Security Officers (CISOs) of FSM and NMHC. This determination and recommendation for an exception will be submitted by the principal investigator to the FSM CISO for final evaluation and determination by the FSM IT Steering Committee, as appropriate.

Data Breach Notification

- 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 **fsmhelp@northwestern.edu.**