ADMINISTRATIVE POLICY

Subject: **Information Security**	Page **1 of 2**	Policy # **Version: 1.0**
Title: **Device Physical Security Policy**	Revision of: **New policy**	Effective Date: **11/15/17**
		Removal Date:

I. PURPOSE

This policy and procedure establishes the required physical attributes of a computing device and its surroundings in order to reduce the risk of unauthorized or unintended disclosure of electronic Protected Health Information (ePHI) and personally identifiable information (PII) from or through the computing device.

II. PERSONS AFFECTED:

All NU FSM faculty, staff and students.

III. POLICY STATEMENT

ePHI and PII displayed on a computing device or which is accessible through the computing device is limited to individuals consistent with a need to know and their specific job responsibilities. For example, this may include data viewed or transmitted through email or access to research data as approved by the data steward or as permitted in the Authorized Personnel List of the NU IRB approved research protocol for that information.

Certain physical attributes to secure a computing device and its surroundings are required, as defined by the Procedure, in order to reduce the risk of unauthorized or unintended disclosure of information.

Computing sessions will automatically lock after a period of inactivity.

Any exceptions to this Policy must be documented in writing and approved by the FSM IT Steering Committee.

IV. PROCEDURE STATEMENT

Computing devices used in offices or lab facilities where patients and study participants congregate or in other physical locations with direct public access will be tethered by a cable lock and screen privacy filter when supported by the device.

Laptops and similar portable computing and storage devices will not be left unattended and unsecured. In addition,

- Use cable locks when supported by the device or the device will be kept in a locked office, desk or cabinet.
- Keep the device on your person but if it must remain in a car keep it locked in a trunk and out of public view.
- In a hotel room the device should be secured with a cable lock or stored in the room safe.
- Devices should not be transported in checked baggage unless required by regulation.

- Portable computer devices and storage media are required to be encrypted at all times.

Entry doors into secure facilities are not be propped open unless all accessible computing devices within that facility are secured and locked.

Contact FSMHELP@northwestern.edu to request a risk evaluation to determine an appropriate approach to computing device security in your particular situation.

V. DEFINITIONS

Computing Device - Desktop, laptop, tablets and other portable computing devices that may display or are permitted access to ePHI and PII.

Data Steward – Representatives from data contributing organizations (e.g., NM) that review and approve data access requests.

VI. POLICY UPDATE SCHEDULE:

Policy review to occur one year after initial implementation and every three years thereafter.

VII. REVISION HISTORY:

11/15/17 – New policy effective.

VIII. RELEVANT REFERENCES:

Rights and Responsibilities for the Use of Central Network and Computing Resources at Northwestern University:
http://www.it.northwestern.edu/policies/responsibilities.html

FSM Security Risk Management Policy:
http://www.feinberg.northwestern.edu/it/docs/Feinberg-IT-Security-Risk-Management-Policy-11_01_17.pdf

FSM Policy on Access to Laboratory Buildings:
http://www.feinberg.northwestern.edu/policies/labs.html

NU Annual Security & Fire Safety Report (includes Campus Security Institutional Policies)
http://www.northwestern.edu/ethics/campus-security/annual-security-report-evanston-chicago.pdf

NU Facilities Management – Locks and Security
http://www.northwestern.edu/fm/services/operation-and-maintenance-services/locks-and-security.html