Subject: **Information Security**	Page **1 of 3**	Policy # **Version: 1.0**
Title: **FSM Device Transfer & Disposal Policy**	Revision of: **New Policy**	Effective Date: **07/01/2019**
		Removal Date:

I. PURPOSE

This policy and procedure establishes the requirements for disposal, re-use, or transfer of Feinberg School of Medicine (FSM) computing devices. These requirements encompass any FSM device which can store non-public data or software licensed by FSM or Northwestern University (NU).

The Health Insurance Portability and Accountability Act (HIPAA) is the basis of this Policy. Specifically, the applicable sections which require implementation include disposal, 164.310(d)(2)(i); and media re-use, 164.310(d)(2)(ii).

This policy augments the FSM General Information Security Policy which defines the minimum standard for handling any form of identifiable health information (e.g. PHI, PII), Disposal of Northwestern University Computers, and NU Office of the Controller, Capital Equipment Disposals & Transfers.

II. PERSONS AFFECTED:

All NU staff, faculty and students that utilize FSM computing devices or storage media that supports FSM education, research or administrative activities.

III. POLICY STATEMENT

FSM devices being re-used within or across FSM or NU departments to different users or to the same user may retain non-public data or licensed software provided that the receiving department or user is authorized to access such data and licensed software. A determination must be made by the individual's supervisors in the sending and receiving departments and documented on a case-by-case basis.

Release of NU or FSM computing devices to another institution, charitable donations or release to an individual requires approval of the FSM Department Administrator or their designee and removal of NU or FSM licensed software and non-public data by FSM IT.

In addition, release of NU or FSM non-public data to another institution requires the approval of Office of Sponsored Research's policy, Research Data: Ownership, Retention, and Access. NU or FSM licensed software is not transferrable.

Computing devices transferred into FSM from other institutions require approval of the FSM Department Administrator or their designee and must be supportable and configurable to FSM IT managed device standards.

NU or FSM computing devices approved for destruction must be erased and unrecoverable and/or destroyed before the device is transferred out of FSM control. FSM maintains procedures that govern the transfer of computing devices to NU for destruction.

Non-reusable electronic media will be sanitized before disposal. Similar to shredding paper reports, CDs and other non-rewritable media must be destroyed before disposal.

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

IV. PROCEDURE STATEMENT

FSM IT will utilize change management procedures (e.g., Footprints) to document the transfer and decommissioning of devices, to document re-deployment rationale (i.e., erase/retain) for data and software on the device and to record approvals. NU email will be part of re-deployment rationale to the extant NU email contains non-public NU data.

Devices approved for decommissioning will be listed on a manifest including description of device, model and serial number. The manifest will accompany the pallet of devices to the NU shipping location and signed off by the dock supervisor as being received. The signed manifest will be recorded in the change management system.

Tools to eradicate stored content without possibility of data recovery will meet the NIST standard, SP 800-88 Rev. 1, Guidelines for Media Sanitization.

V. ROLES AND RESPONSIBILITIES

FSM IT Security will provide policy oversight, direction and reporting regarding compliance.

Custodians, owners and users will be responsible to ongoing compliance with this Policy.

VI. POLICY UPDATE SCHEDULE:

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

VII. REVISION HISTORY:

07/01/19 – New policy effective.

VIII. RELEVANT REFERENCES:

FSM General Information Security Policy:
https://www.feinberg.northwestern.edu/it/docs/General-Security-Policy-092216-V2-1.pdf

Health Insurance Portability and Accountability Act (HIPAA):
http://www.hhs.gov/hipaa/for-professionals/index.html

Guidelines for Media Sanitization, SP 800-88 Rev. 1:
https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

Research Data: Ownership, Retention, and Access:
http://research.northwestern.edu/sites/research/files/policies/Research_Data.pdf

Disposal of Northwestern University Computers:
http://www.it.northwestern.edu/policies/disposal.html

NU Office of the Controller, Capital Equipment Disposals & Transfers:
https://www.northwestern.edu/controller/accounting-services/equipment-inventory/disposals.html

NU Data Access Policy:
https://www.it.northwestern.edu/policies/dataaccess.html

FSM Authorization & Access Control Policy:
https://www.feinberg.northwestern.edu/it/docs/access-control-policy-02.28.18.pdf

FSM IT Request Forms:
http://secure.feinberg.northwestern.edu/it/forms/index.html