National University of Health Sciences
General Policies

Title: **HIPAA Endpoint Data Security Procedures and Removal of PHI or Sensitive Data from Premises**

Date Adopted: **02/01/18**

Date(s) Revised:
Date(s) Reviewed: 09/29/2020

President J. Trujillo

09/29/2020
Date

POLICY STATEMENT

The following policy addresses administrative security for mobile endpoints and removal of PHI or Sensitive Information from NUHS's premises.

SCOPE

All personnel.

DEFINITIONS

Endpoint: Mobile devices including but not limited to laptops, smartphones, or other portable electronic equipment capable of storing PHI and/or Sensitive Information.

Personnel: Includes, but is not limited to, all employees, medical and clinical staff, business associates, allied health professional staff or students, vendors, volunteers, excluding patients and visitors.

PHI: Individually identifiable health information, including patient demographics, that is created or received by a provider and identifies the person and relates to his or her past, present, or future physical or mental health, treatment, and/or payment, except for information relating to persons who have been deceased for more than fifty (50) years.

Sensitive Information: Data that is proprietary to NUHS and is not intended to be disclosed to the general public.

PROCEDURE

- PHI and Sensitive Data shall not be removed from NUHS's premises without the prior authorization of the HIPAA Security Officer. This authorization may be a one-time authorization or may be applicable to particular job types. The following job types and individuals are expressly authorized to remove PHI and Sensitive Data:
    - Persons transporting data to or from post offices or other repositories;
    - Business Associates for and in their capacity as such pursuant to valid Business Associate Agreements;
    - Foot Levelers;
    - Clinical personnel in the exercise of their professional judgment;
    - Administrative personnel and leadership in the exercise of their professional judgment.
- All laptops and smartphones shall employ full-disk encryption or password protection upon shutdown or restart.
- All personnel must power down all endpoints (other than smartphones) containing PHI or Sensitive Data prior to transporting such data offsite.

POLICY RESPONSIBILITY

HIPAA Security Officer

REVISION

NUHS reserves the right to unilaterally revise, modify, review or alter the terms and conditions of the policy within the constraints of law, with or without reasonable notice.