National University of Health Sciences
General Policies

Title: **HIPAA Technical Safeguards – User IDs and Emergency Access**

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

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

President J. Stuffel

Date 9/29/2020

POLICY STATEMENT

The following policy addresses the implementation of discrete User IDs and emergency access to records containing PHI or Sensitive Information.

SCOPE

All personnel.

DEFINITIONS

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.

REGULATORY REFERENCE

45 C.F.R. 164.312(a).

PROCEDURE

- PHI and Sensitive Information are located in the following networked electronic repositories:
  - NUHS Network and Devices
  - Athena
  - Medisoft
  - Copiers and Fax Machines

- Each of these networks requires the utilization of a unique user ID assigned by the network administrator. For example, in the case of the NUHS, the user ID is assigned and maintained by the HIPAA Security Officer. In the case of the Athena software, it is assigned and maintained by third party software provider. [Medisoft, and all copiers and fax machines are fully maintained by NUHS and as such, user IDs and access is granted by the HIPAA Security Officer or device has an encrypted drive.]

- In cases where emergency access is required to PHI residing on any of these systems, the first point of contact shall be the HIPAA Security Officer at [630-889-6606]. In the event the HIPAA Security Officer is unavailable, the second point of contact shall be the HIPAA Privacy Officer at [630-889-6513]. If both are unavailable, [630-889-6604].

- For each third party provider (i.e., Athena), the initial point of contact concerning emergency access shall be the HIPAA Security Officer followed by the HIPAA Privacy Officer.

- These individuals will then evaluate the request as follows:
  - First, the party will evaluate whether the request is legal and compliant with existing state and federal privacy law.
  - Second, the party will evaluate whether a genuine emergency exists.
  - Assuming the answer to both questions is "yes," and assuming that the evaluating party has had the opportunity to consult with counsel if reasonable under the circumstances, emergency access may be granted.

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.