National University of Health Sciences
General Policies

Title: **HIPAA Technical Safeguards – Transmission Security**	Page **1** of **2**
Date Adopted: **02/01/18**	Date(s) Revised: Date(s) Reviewed: 09/29/2020
President	09/29/2020 Date

POLICY STATEMENT

The following policy addresses electronic transmission security controls for PHI.

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(e).

PROCEDURE

- All PHI transmitted in electronic format shall be encrypted in transit using secure socket layer or other commercially reasonable technology, including encryption technology provided in email and file transfer systems.

- All PHI stored in electronic format shall be encrypted at rest when possible. Reference is made to Administrative Safeguard Procedures addressing encryption at rest for mobile endpoints.

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.