





National University of Health Sciences General Policies

Title: HIPAA Contingency Plan for Systems Containing Sensitive Information or PHI		Page	1	of	2
Date Adopted:	02/01/18	Date(s) Revised:			
		Date(s) Reviewed:	09/29/2020		
President		Date			

POLICY STATEMENT

The following required contingency plans will be implemented to provide for required data recovery and remediation.

SCOPE

IT Department (all locations).

DEFINITIONS

Contingency: One or more natural or manmade events that result in the denial of access, deletion, or loss of Sensitive Information or PHI on a temporary or permanent basis, including but not limited to any damage to systems containing PHI.

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. 163.308(a)(7).

PROCEDURE

- Under the guidance and leadership of the HIPAA Security Officer and MIS department within NUHS shall implement the following procedures for addressing Contingencies:
 - NUHS shall routinely back up available data by through the use of data backup services provided by their contract vendor Gordon Flesch.
 - NUHS shall develop and document a disaster recovery plan consisting of the following: In case of severe device failure, security officer with contact vendor Gordon Flesch to restore function.
 - The continuation of clinical functions and patient care shall be at all times the first priority in the resumption of services following a Contingency. The HIPAA Security Officer shall supervise emergency mode operations and disaster recovery.

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.