VERA Z. DWYER COLLEGE OF HEALTH SCIENCES
INDIANA UNIVERSITY SOUTH BEND

TITLE: Division of Dental Education Dental Hygiene Clinic HIPAA Policy

POLICY NO: IUSB-CHS-DE.003

EFFECTIVE DATE: January 1, 2018

TARGET GROUP: Division of Dental Education Students

SECTION: Division of Dental Education Student Policy

REVISION DATE: December 15, 2017

Purpose:

The purpose of this policy is to define the department procedures and policies for handling Protected Health Information (PHI) in compliance with Health Insurance Portability and Accountability Act (HIPAA).

Policy:

The Dental Hygiene Clinic at IU South Bend treats the public 10 months a year. The data collected on each patient is stored in the Dentrix Enterprise System. UITS maintains the system and server, which is housed in the IUPUI Data Center.

- All PHI must be maintained in a secure digital or paper format
  - This includes heavily encrypted, maintained digital environment or keeping patient paper files in a locked cabinet in a locked office
- The department destroys any unneeded documentation by cross-cut shredding or through the University shredding program
- The clinic manager has a monitor screen on both workstations at the front desk.
- Students lock their computers prior to walking away from their clinical unit.
- Students are not permitted to share passwords, or to sign in for any other person.
- All computers are set by UITS to time out after 90 minutes of inactivity (exception to policy form on file).
- The x-ray suite computers are logged off immediately after finishing radiographs on patients.
- Faculty and the clinic manager walk through the clinic to verify all computers are logged off, but kept on for updates.
- All computers have a sign “Don’t forget to log off!”

Security policies

Because the dental hygiene clinic is open to the public PHI should never be displayed without taking precautions to protect the information. The clinic shall remain locked during non-business hours to facilitate protection of the information. Key card access is required from the inside of the building. The outer doors are set to automatically lock during off hours. All other doors to the clinic are also kept locked routinely.

The Program Director (PD) serves as the HIPAA liaison for the department. The PD monitors training of faculty, staff and students. Training is done through One.iu E-training or face to face.

Attestation/training files are kept in the department, and sent to HIPAA Compliance when appropriate.

No patient information data will be stored on any terminal, computer, or person. Faculty are permitted to use unmarked patient files for teaching purposes, but no patient information is stored with those files; Dentrix and MiPacs removes all PHI prior to saving the images in a jpeg format.

As soon as a resignation or hiring occurs in the department faculty, secretary, or clinic manager position, the PD will revoke access.

The policies and procedures are located on the department H drive and all faculty and staff have access to them. These are updated annually and shared with faculty and staff.

In the case of a security breach, UITS HIPAA Security Officer and Compliance Office would be notified immediately for assistance.