Policy Title:	Health Information Security
Policy Number:	STUD-305
Revision Date:	May 2019
Policies Superseded:	1811; STUD-111
Policy Management Area(s):	Student Affairs

SUMMARY

All medical information, including but not limited to health care charts, will be maintained in a safe, secure environment with limited access to ensure confidentiality and to protect against loss and unauthorized use.

POLICY

I. PURPOSE

To protect all health information, in line with University policy UNIV-483 Data Privace, Classification, and Protection.

II. PROCEDURE

A. All patient records are maintained in a physically secure area, preferably in a centralized location. Access is limited to authorized personnel.

B. Health records will be kept in secure areas at all times. Health records will not be left unattended in areas where unauthorized individuals could gain access.

C. All health records that are placed in the shred bins under the medical records desk must be collected daily and placed in the secure locked shredding container at the end of each shift. These records are destroyed by a bonded and insured shredding company that picks up and shreds on site as per University contract.

D. All health records must be returned to medical records within twenty-four (24) hours of a patient's visit.

E. Original records should not leave Student Health Services except in response to a properly executed subpoena or court order.

F. Secondary records which are by-products of the original record are protected with the same diligence as the original health record. Secondary records include other health information maintained by the facility in which the patient and/or provider are individually identifiable (i.e. billing information).

G. Inactive billing records containing diagnoses or coded data should be maintained in a locked area where only medical record personnel have access.

H. Access to electronic health records are controlled using security passwords and are used by authorized personnel only. In addition, computer monitors are protected by using privacy screens.

I. Failure to abide by security procedures may result in personal liability and sanctions, up to and including termination.

J. A protected health information (PHI) security audit is done nightly to ensure confidentiality and to protect against loss and unauthorized use.