SUMMARY

All medical information will be maintained in a safe, secure environment with limited access to ensure confidentiality and to protect against loss and unauthorized use.

I. Purpose

To protect all health information.

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

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

E. Secondary records which are by-products of the original record should be 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.

F. Inactive billing records containing diagnoses or coded data should be maintained in a locked area where only medical record personnel have access.
G. Access to computer files are controlled using security passwords and are used by authorized personnel only. In addition, computer monitors are protected by using privacy screens.

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

I. A protected health information security audit is done nightly to ensure confidentiality and to protect against loss and unauthorized use.