Oklahoma State University

Title: Data Backup and Storage	**Policy #: SEC-11.03**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.310(d)(2)(iv)**
Standard: Device & Media Controls	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Pages: Page 1 of 2**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PURPOSE:

Ensure continued operations in the event of a natural disaster, equipment failure and/or accidental removal of files and support the need to retrieve archived information.

POLICY:

OSU will create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. *§164.310(d)(2)(iv)*

Measures will be taken to create backup copies of all mission-critical data utilized on the network. Mission-critical data is defined as any user-generated data or file configurations stored on the production network. Methods are implemented for authorized users to gain access to the backup data quickly. These procedures are updated to coincide with changes within the Center for Health Sciences and OSU Tulsa. Offsite storage is utilized for critical tapes and documentation. Access to the offsite storage and contents is documented and understood by responsible Information Technology personnel

PROCEDURE:

Responsibility of Information Technology
Two employees from each campus are assigned the responsibility of ensuring the completeness of the backup process each day, reporting any failures and taking appropriate action to correct any problems. One will have the primary responsibility of performing this function on a daily basis and the other will complete the operation in the absence of the primary.

One complete backup excluding the system drive will be captured after close of business on Friday followed by four incremental backups after close of business Monday through Thursday. Systems drives will be copied to tape when a server is installed and/or patches are applied. Full backups are completed on the email servers and clinical medical servers each night.

Information Technology personnel will ensure that every Saturday morning a full backup is done on certain parts of each server, this may include all or part of each respective server. Sunday through Friday, incremental backups will be done. All backups will be retained for one (1) year. January's backup is to be retained for seven (7) years. At the first of every month full backups are to be done. All servers are housed in the OSU-Tulsa campus, all backup devices are housed at CHS, as a result, the off-site storage is already

in place. The remaining incremental tapes are reused every 90 days. Full backup tapes are reused every 32 days. A paper log will be kept stating which tape(s) are pulled noting the tape name, serial number and date.

A list of devices and drives can be found in the Information Technology Operating Manual under Backup Schedule.

Responsibility of User

The user is responsible for maintaining copies of data stored on users' computers. In the event that a data file needs to be restored the user must call or email the help line with the request. The restoration of the file(s) will be completed within a 24-hour time frame. There is to be no PHI stored on the user's computer. If a user request's a restoration of a file that does contain PHI, the HIPAA Compliance Office will be notified immediately, and the user may receive appropriate training and/or sanctions if necessary.