# UNC School of Medicine
# Electronic Data Disposal Policy

## OVERVIEW

A huge volume of electronic data is being transmitted and stored on computer systems and electronic media by virtually every person conducting business in the School of Medicine. A large percentage of that data contains sensitive information, including personnel records, financial data, and protected health information. Users need to understand that simply deleting data from media does not permanently remove the information. Deleted files are susceptible to unauthorized retrieval if not disposed of properly. As such, all users of computer systems within the School of Medicine (SOM), including contractors and vendors with access to SOM systems, are responsible for taking the appropriate steps, as outlined below, to ensure that all computers and electronic media are properly sanitized before disposal.

## PURPOSE

The purpose of this policy is to establish a standard for the proper disposal of media containing electronic data. The disposal procedures used will depend upon the type and intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

## SCOPE

The scope of this policy includes all electronic media in the School of Medicine and all personnel who are responsible for or who use School of Medicine computer systems. Vendors and contractors who have access to School of Medicine computer systems are also subject to this policy.

## POLICY

### General

All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.

1) Overwriting hard drives for sanitization: Overwriting is an approved method for sanitization of hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) and zeros (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., "11111111" followed by "00000000") the magnetic fluxes will be physically changed and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge the hard drive requires overwriting with a pattern, and then its complement, and finally with another pattern (e.g., overwrite first with "00110101 ", followed by "11001010", then "10010111"). Sanitization is not complete until the three overwrite passes and a verification pass are completed. A variety of

software packages are available on the open market that properly performs this function. Examples include, but are not limited to, “Killdisk” and Semantec’s “Gdisk” (part of the Ghost product).

2) Destruction of electronic media: Destruction of electronic media is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the media such as a computer, tape reader, audio or video player.

3) Clearing data: Clearing data such as formatting or deleting information removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. Because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing media intended for disposal outside of the School of Medicine

## Disposal of Hard Drives

1) Disposal of hard drives to other departments or outside of the School of Medicine: Prior to disposal, operable hard drives must be overwritten in accordance with the procedures in paragraph A1 above. The owner must be able to certify that the hard drive was properly sanitized. Written certification should include the make, model, and serial number of the hard drive and the date that the procedure was performed. Equipment designated for surplus or other disposal must have a label affixed stating that the hard drive has been properly sanitized. The label should be a high visibility color that is easily recognizable.

2) Transfer of hard drives within a department: Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. It is recommended that all electronic media be sanitized per paragraph A1; however, since the media is remaining within the department, the hard drive may instead be formatted prior to transfer. Since, special recovery tools must be used by an individual to access the data erased by this method any attempt by an individual to access unauthorized data would be viewed as a conscious violation of HIPAA regulations and the School of Medicine Confidentiality Statement.

3) Sending a hard drive out for repair or for data recovery: The vendor repairing or recovering data on the hard drive must have signed an appropriate Business Associate Agreement with the School of Medicine or UNC Health Care System, stating that they will take proper care of the data. Once data is recovered or the hard drive is repaired the original hard drive must be returned to the owner so that the owner can dispose of it per this School of Medicine policy for proper disposal of hard drives.

4) Repairing a hard drive under warranty: In the special situation where a hard drive under warranty has failed and the manufacturer requires that the failed disk drive be returned, an appropriate Business Associate Agreement between the manufacturer and the School of Medicine or UNC Health Care System must be in place before the drive can be shipped to the manufacturer. If the manufacturer will not sign a Business Associate Agreement, then the old drive must be properly destroyed and the owner of the system must cover any costs associated with purchasing a new drive.

5) Disposal of damaged or inoperable hard drives: The owner must first attempt to overwrite the hard drive in accordance with the procedures in paragraph A1 above. If the hard drive can not be overwritten, the hard drive must be disassembled and mechanically damaged so that it is not usable by a computer.

## Disposal of Electronic Media Other Than Hard Drives

1) Transfer of electronic media other than hard drives within a department:
Before electronic media is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be reformatted if the media type allows it or erased if formatting is not possible.

2) Disposal of electronic media outside of the School of Medicine: All electronic media other than computer hard drives must be rendered unusable before leaving the School of Medicine. Use of certified commercial disposal systems such as “Shred-it” is encouraged.

DEFINITIONS

1) Electronic Media – Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, USB drives, memory sticks, MP3 players (iPod), Personal Digital Assistants (PDA’s), digital cameras, smart phones and tapes.

2) Sensitive Information - Sensitive information is classified as Protected Health Information (PHI), Confidential Information or Internal information as defined in the UNC Health Care Information Security policy. For a full description of security classifications, refer to the UNC Health Care Information Security policy.

3) Sanitization – To expunge data from storage media so that data recovery is impossible. The most common types of sanitization are destruction, degaussing, and overwriting.

## Violation of Policy

If it is suspected that the proper procedures as outlined in this policy for disposing of electronic media have not or are not being followed, report the incident to the Information Security Officer. If improperly sanitized electronic media is found, give the media to the Information Security Officer.

## Enforcement

Any person found to have violated this policy will be subject to appropriate disciplinary action.

Approved by the HIPAA Planning and Oversight Council (HPOC): March 4, 2003

REVISION HISTORY
September 16, 2005