University of South Carolina
School of Medicine
Electronic Data Disposal Policy

I. OVERVIEW

A large volume of electronic data is stored on computer systems and electronic media by virtually every person conducting business in the School of Medicine. This data may contain sensitive information, including personnel records, financial data, and protected health information. Improper disposal of these non-volatile storage devices or the data contained therein may result in unauthorized access constituting a security breech. As such, all users of computer systems within the School of Medicine (SOM) are responsible for ensuring the proper use and disposal of these devices. Electronic Media is defined as any non-volatile, electronic storage device that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks, videotapes, audiotapes, and removable storage devices such as floppy disks, zip disks, CD's, DVD's, and USB memory devices.

II. 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.

III. 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.

IV. POLICY

A. General

All non-volatile electronic media must be properly "cleaned" of all sensitive/confidential information before it is transferred from the custody of its current owner. The proper methods utilized depend 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 entails replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable if appropriate software is utilized. Overwriting consists of writing a pattern of ones (1) and zeros (0) onto the device effective erasing the previous data. Sanitization is not complete until the three overwrite passes and a verification pass are completed. Software approved by the Office of Information Technology must be utilized after proper training.

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.

B. Disposal of Hard Drives

1) Disposal of hard drives to other departments or outside of the School of Medicine: Prior to disposal, all non-volatile media must be removed from the device and 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 University Specialty Clinics, stating that they will assume responsibility of maintaining confidentiality. Once data is recovered or the hard drive is repaired the original hard drive must be returned to the owner for proper disposal as noted herein.

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 University Specialty Clinics must be in place before the drive can be shipped to the manufacturer.

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.

C. 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.

D. 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.

V. Enforcement

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