Media Disposition Procedures

1. Use of sanitizing software

   a. Each department should assign a responsible party to oversee the sanitization process. As this is a technical process the department LSP is recommended by ISTM as the person who should be responsible for the sanitation of the department's electronic media.

   b. Only a software package approved by the IU Security Office (ITSO) or ISTM will be used to overwrite any IUSM electronic media requiring disposition. For more information on recommendations and procedures from the ITSO please review their "How to Securely Remove Data" document. ITSO recommends using the Symantec "Gdisk" software, available on the IUWARE web site.

   c. Additionally, the Department of Defense (DOD) standard for disposition of unclassified computer hard drives recommends several different software packages that comply with the standards required by both the DOD and IUSM policy. They are:

      * "No Trace" software developed by Communication Technologies, Inc., [www.comtechnologies.com](http://www.comtechnologies.com).
      * "Data Eraser" software developed by On Track Data International, Inc., [www.ontrack.com](http://www.ontrack.com).
      * "UniShred Pro" software developed by Los Altos Technologies, [www.lat.com](http://www.lat.com).
      * "WipeDrive" software developed by Access Data Corporation, [www.accessdata.com](http://www.accessdata.com).
      * "InTether Sanitizer" software developed by Infraworks, [www.infraworks.com](http://www.infraworks.com).

   d. DOD Standard 5220.22-M requires a minimum of three separate overwrites of the electronic data. Each software package has a particular setting that forces this level of sanitization. The individual using the software package should verify this setting is in place before the sanitization process begins.

2. Physical destruction of the electronic media

   a. Soft electronic media such as floppy disks and CDs should be destroyed so that the media cannot be reconstructed. Cutting the floppy disk in half with a pair of scissors is neither an adequate nor appropriate means of destruction. ISTM has purchased a shredder capable of shredding CDs and floppy disks. You are welcome to use the shredder in our offices to destroy media. Please contact ISTM at 278-8751 to schedule time to use the shredder.

   b. Electronic media such as hard drives normally do not require physical destruction to sanitize them prior to disposition. In the event the hard drive does not properly work or the sanitation cannot be guaranteed through means of using software then the hard drive can be destroyed using one of two methods:
An approved company capable of adequately destroying hard drives can be contracted to provide this service. This company must have a signed Business Associates Agreement on file with ISTM and the department contracting the service in order to properly dispose of the electronic media.

The hard drive can be physically destroyed by the department. Any department wishing to physically destroy a hard drive can utilize the following process:

a. Remove the hard drive cover to expose the platters inside.
b. Drill holes through the platters. Remember to wear appropriate eye protection.
c. Remove the platters from the drive.
d. Dispose of the platters and other pieces of the hard drive.

3. Documentation of sanitation or destruction of electronic media

a. Once the sanitization or destruction is complete, the Originating User will certify in writing that the data on the electronic media has been processed for sanitation.

* For hard drives that have been sanitized and will be turned in for disposition, use the IUPUI Purchasing Department's hard drive wipe form available at: www.purchasing.iupui.edu/surplus/cpu.cfm.

* For removable media, ISTM recommends the department develop a local form to maintain a record of the disposition for all removable media containing sensitive data such as patient data. An example of one type of local form can be found here: Sample Removable Media Disposition form.