BOSTON UNIVERSITY

	Title:	Device and Media Control Policy
	Policy ID:	BU-100-003
	HIPAA Section:	164.310(d)
	Version:	1.0
	Effective Date:	April 20, 2005
Policy Custodian:	Information Services & Technology	
Authorized By:	Vice President for Information Services & Technology	

1. Purpose – To implement policies and procedures governing the receipt, movement, and removal of hardware, software, and electronic media that contain electronic Protected Health Information (ePHI) into, out of, and within Boston University's facilities. This policy relates to disposition and reuse of hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards, memory sticks, and all other forms of media and storage devices.

2. Device and Media Control Policy – All ePHI must be permanently removed from these devices before the devices can be discarded or re-used. The movement of devices containing ePHI into, out of, and within the Covered Entities (CEs) must be tracked and logged.

2.1. Disposal [164.310(d)(2)(i)] – CEs must ensure that devices or media do not contain ePHI before disposing of such devices or media. The device or media must be physically destroyed if it contains ePHI.

2.1.1. Destruction of all electronic media and information systems containing ePHI must be tracked and logged, recording the following information:

- Date and time of destruction
- Who performed the destruction
- Brief description of media or information systems that was destroyed

2.2. Media Re-Use [164.310(d)(2)(ii)] – CEs must ensure that devices or media do not contain ePHI before reuse of such devices or media. If the device or media contains ePHI, the CE must use a data destruction tool approved by the IS&T Information Security group to permanently remove the ePHI. Reformatting a disk is not sufficient.

2.2.1. The use of a data destruction tool before reuse is not required if the media is used for system or data backup, as long as the media is stored and transported in a secured environment.

2.3. External Movement of ePHI – The following procedures must be followed for the transport of storage media with ePHI outside of a CE.

2.3.1. The ePHI must be encrypted before being moved outside a CE.

2.3.2. All media with ePHI transported outside of a CE must be new, or if previously used to store unencrypted ePHI, it must be certified by IS&T Information Security group as having all residual data removed or obliterated.

2.3.3. Instructions for the return of the media must be agreed to in writing before the media are transferred to others. Do not rely on other parties to destroy or obliterate media.

2.4. Accountability [164.310(d)(2)(iii)] – CEs must implement a procedure to track and maintain records of the internal and external movement of storage devices and media containing ePHI. Tracking includes recording the chain of custody and each party responsible for the device or media while in transit.

2.5. Data Backup & Storage [164.310(d)(2)(iv)] – CEs must make an exact retrievable copy of the ePHI before relocation of a storage device or media containing ePHI, if the device or media contains the last remaining copy of ePHI.

Modification Control Sheet

Rev	Date	Author	Description of Modification
0.0	20100429	David Hutchings, IS&T Information Security	Changed all references to “University Information Systems” and “Information Systems and Technology” to “Information Services & Technology”.