BOSTON UNIVERSITY

BOSTON UNIVERSITY	**Title:**	Facility Access Control Policy
	Policy ID:	BU 100-000
	HIPAA Section:	164.310(a)(1)
	Version:	1.1
	Effective Date:	April 29, 2010
Policy Custodian:	Information Services & Technology	
Authorized By:	Vice President for Information Services & Technology	

1. Purpose – To control, monitor, and limit physical access to the information assets of Boston University's Covered Entities (CEs) and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

2. Facility Access Controls [164.310(a)(1)] – It is the responsibility of the CEs to protect their ePHI by controlling and monitoring physical access to their sites. Physical access to University data centers will be controlled and monitored by the data center staff.

2.1. Contingency Operations [164.310(a)(2)(i)] – CEs must have procedures that allow access to facilities by appropriate personnel during a disaster or declared emergency situation to facilitate the retrieval of the back-up media, hardware, and software necessary for the recovery of systems and restoration of lost data. See the Disaster Recovery and Contingency Planning Policy [BU 000-006].

2.1.1. The Facility Security Plan and controls will not prohibit building access to authorized disaster recovery personnel retrieving media, systems, software, or hardware necessary for the recovery of critical information systems during a declared emergency mode situation or following a disaster. Physical access by individuals retrieving back-up media should be logged whenever feasible. Logs should include name of person, date, materials removed, and other appropriate details.

2.1.2. Emergency Access Procedures – Whenever possible, emergency personnel should be escorted by a guard or another authorized person. Physical access by emergency personnel should be logged whenever feasible.

2.2. Facility Security Plan [164.310(a)(2)(ii)] – CEs must implement procedures to protect their facilities and equipment from unauthorized physical access, tampering, or theft.

Each CE must develop a Facility Security Plan specific to its local environment.

2.2.1. The physical security of any site containing ePHI resources will be periodically reviewed by Boston University's Information Security group with the assistance of the CEs and appropriate support personnel, especially after any

significant change that may have affected the security of data and applications resident at that site.

2.2.2. Property Control

2.2.2.1. Inventory – An inventory of information resources that access or contain ePHI will be maintained by the CE. A reconciliation of the information resources inventory should take place annually.

2.2.2.2. Security – Information resources must be kept in locked spaces, rooms, or cabinets. Information resources that contain ePHI must be located only where physical access to the device can be controlled and monitored.

2.2.2.3. Inspection of Packages, etc. – All packages, bags, briefcases, etc. are subject to inspection both upon entry to and exit from Boston University buildings.

2.2.3. Classification for Physical Access Control – CE information resources may require additional physical protection beyond that which is provided by a controlled access building. For the purposes of this section, the physical area housing a CE's information resource is divided into four separate classifications.

2.2.3.1. University Data Centers – A University data center is a restricted area devoted to housing computer equipment that may store or process ePHI. All access will be restricted to authorized persons only and must be logged.

2.2.3.2. Network Wiring/Communications Closets – These locations house network termination equipment including switches and routers. Doors will be kept locked and key distribution limited to prevent unauthorized access to network gear.

2.2.3.3. Locked Location – A locked location can be a workspace with a door which remains locked when not attended. It can also be a locked cabinet, drawer, closet, or resource room, depending on the size of the equipment that is being secured. Systems that store or process ePHI for a small group of users within the area may be located here. All access to the locked area must be restricted to authorized persons only.

2.2.3.4. Non-secured Location – A non-secured location can be a workspace that may or may not be locked. Systems that store or process ePHI for individual use (e.g., a desktop) within the area may be located here. Additional physical safeguards must be employed to compensate for the absence of facility controls.

2.3. Access Control and Validation Procedures [164.310(a)(2)(iii)] – All CE occupied buildings must have controlled access into the building. If the building is not totally occupied by the CE, access must be controlled to those portions of the building housing the CE. Access control must be effective 24 hours a day, seven days a week. Acceptable methods for controlling access include key-locked or attended entrances and keyed physical access cards. CEs must implement procedures to control and validate a

person's access to facilities based on their role or function, including visitor access control. CEs must also implement procedures for control of access to software programs for testing and revision. These procedures will be contained in the CE's Facility Security Plan.

2.3.1. Additional controls are as follows:

2.3.1.1. Entrances and exits that are not guarded or attended must remain locked at all times and must have automatic closers. Doors must not be propped open.

2.3.1.2. The access control procedures in place must be followed by each person entering a controlled access facility. Personnel with access to restricted areas must not allow unauthorized individuals access those restricted areas. Personnel must be vigilant and challenge and report unidentified persons who have gained, or seek to gain, access.

2.3.1.3. All access to University data centers must be logged. Where automated logging systems (card access systems) do not exist, logging must be done manually. Logs should include name of person, date, and other appropriate details.

2.3.1.4. When practicable and depending on the value and sensitivity of the equipment and data housed in the building, entrances, exits, windows and other means of access into the building should be wired for alarms.

2.3.1.5. When practicable and depending on the value and sensitivity of the equipment and data housed in the building, entrances, exits and strategic areas of the building should be monitored.

2.4. Maintenance Records [164.310(a)(2)(iv)] – Each CE is responsible for ensuring that all repairs, modifications, and maintenance performed on the physical access controls of its facilities are tracked and logged. The physical security controls include doors, locks, fences, badge readers, and surveillance equipment.