BOSTON UNIVERSITY

BOSTON UNIVERSITY	**Title:**	Disaster Recovery and Contingency Planning Policy
	Policy ID:	BU 000-006
	HIPAA Section:	164.308(a)(7)
	Version:	1.0
	Effective Date:	April 20, 2005
Policy Custodian:	Information Services & Technology	
Authorized By:	Vice President for Information Services & Technology	

1. Purpose – To ensure that electronic Protected Health Information (ePHI) is protected from disasters including, but not limited to, floods, fires, vandalism, and failures of hardware or software. Formal procedures must exist to ensure the recoverability of ePHI and resumption of critical business processes following a disaster.

2. Contingency Plan [164.308(a)(7)] – Contingency Planning is the recognition of the possibility of a future disaster including the development, and periodic updating, of detailed plans that provide an agreed level of interim information processing, should a disaster occur. Included in Contingency Planning are procedures to ensure the successful recovery of critical business and information assets following a disaster.

2.1. Data Backup Plan [164.308(a)(7)(ii)(A)] – To ensure the recoverability of ePHI and other critical information assets, Boston University Covered Entities (CEs) must maintain formal data backup procedures.

2.2. Disaster Recovery Plan [164.308(a)(7)(ii)(B)] – Managers assigned responsibility for a system or application are required to ensure the development of the Disaster Recovery Plan (DRP) for that system or application. A system is defined as the collection of application software required to perform a specific function. The organization responsible for a system or application should not accept the system or application for processing without a coordinated disaster recovery classification and an approved DRP (See section 2.5 for more information related to disaster recovery classification.)

2.2.1. The DRP must be structured to ensure restoration within the time period for the disaster recovery classification assigned to that application.

2.2.2. When developing DRPs, planners must consider the disaster so catastrophic as to prohibit processing in the original processing center for an extended period.

2.2.3. Restoration times must be agreed to by both the organization processing the system or application and the user organization(s) before the restoration times are documented in the DRP. These times should be determined by the Risk Analysis.

2.2.4. Copies of the DRP must be readily available to appropriate personnel in the event of an emergency. Specifically, copies should be maintained in secure locations at the normal processing site, the contingency processing site(s), and at an off-site storage location.

2.2.5. Responsibility for DRP and Emergency Operations Plan Development – The HIPAA Security Officer is ultimately responsible for coordinating the development of the DRP and Emergency Operations Plan.

2.3. Emergency Mode Operation Plan [164.308(a)(7)(ii)(C)] – Formal procedures must be developed to enable the continuation of critical healthcare processes and the protection of ePHI while operating in emergency mode. Examples of situations that may trigger emergency mode operations include but are not limited to: bomb threat, civil disturbance, communications failure, earthquake, explosion, fire, flood, gas/chemical leak, hurricane/wind storm, medical emergency, noxious fumes, power failure, strike, terrorist activity, and workplace violence.

2.4. Testing and Revision Procedures [164.308(a)(7)(ii)(D)] The DRP and Emergency Operations Plan must be tested if appropriate to do so and updated whenever changes occur that affect the system or application. This includes, but is not limited to changes in personnel, procedures, hardware, and software.

2.4.1. At a minimum, an annual review must be conducted and documented by the responsible manager to determine if the plan needs to be revised.

2.4.2. The frequency of the reviews should be commensurate with the criticality of the asset or function protected as determined by the criticality analysis. Contact lists must be reviewed quarterly.

2.4.3. All major changes require approval by the HIPAA Security Officer

2.5. Applications and Data Criticality Analysis [164.308(a)(7)(ii)(E)] – All systems and applications are important to the University. Should a catastrophic disaster occur in any of Boston University CE's processing centers, there are certain applications that will prove to be of the utmost importance to ensure operational continuity at the CEs. The table below defines the classification structure for applications processed in Boston University Covered Entity processing centers.

System/Application Priority Classifications for Disaster Recovery Purposes (Example)

Category	Class	Description	Restore Time
1	Vital	Functions, systems, and applications that are absolutely essential for CEs to remain operational and to provide necessary services to our users.	24 to 144 hours after a disaster is declared
2	Critical	Functions, systems, and applications that are essential for CEs to remain operational.	5 to 11 days after a disaster is declared. Restored concurrently or following the completion of Category 1 items.
3	Essential	Functions, systems, and applications that enhance operations, but are less time critical	11 to 18 days after a disaster is declared
4	Valued	Functions, systems, and applications that are not deemed vital, critical, or essential.	After Category 1, 2, and 3 have been restored

2.5.1. A Business Impact Analysis (BIA) must be performed and documented in order to classify a system/application for disaster recovery purposes. The BIA is designed to describe the impact on CEs if the system/application cannot operate due to a major disaster in any one of Boston University's processing centers.

2.5.1.1. Representatives of the application owner, application support, and platform support organizations must complete the BIA as early as possible in the development life cycle of the system/application.

2.5.1.2. They must select an appropriate disaster recovery category based upon the criteria in the Priority Classification Table above. An elaborate analysis is not required, however, the results must support the classification requested. Document any assumptions made.

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”.