


## BOSTON UNIVERSITY

|   |  |                        |                             |
|---|--|------------------------|-----------------------------|
|  |  | <b>Title:</b>          | Security Management Process |
|   |  | <b>Policy ID:</b>      | BU 000-001                  |
|   |  | <b>HIPAA Section:</b>  | 164.308(a)(3)               |
|   |  | <b>Version:</b>        | 1.0                         |
|   |  | <b>Effective Date:</b> | April 20, 2005              |
| <b>Policy Custodian:</b>  | Information Services & Technology                    |                        |                             |
| <b>Authorized By:</b>   | Vice President for Information Services & Technology |                        |                             |

1. Purpose – To describe the overall process for managing the Policies, Standards, and Procedures established by Boston University to ensure the prevention, detection, containment, and correction of security violations in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The HIPAA Security Rule focuses specifically on the confidentiality, integrity, and availability of protected health information in electronic format (ePHI.)

2. Security Management Policy – Boston University will protect the confidentiality, integrity, and availability of ePHI by maintaining appropriate safeguards for the networks and systems that handle ePHI. Boston University will implement policies and procedures to prevent, detect, contain, and correct security violations. Boston University will use processes and safeguards including, but not limited to, the following:

2.1. Risk Analysis [164.308(a)(1)(ii)(A)] To gauge and document reasonably anticipated threats to ePHI and vulnerabilities in systems that deal with ePHI. An ePHI risk analysis will be conducted periodically or whenever significant changes that could alter the security posture of the Covered Entities (CEs) are planned or made to the environment. See the Risk Analysis Policy [BU 000-001A].

2.2. Risk Management [164.308(a)(1)(ii)(B)] Processes and controls will be implemented and maintained to safeguard ePHI from the risks identified in the Risk Analysis. Risk and vulnerabilities will be reduced to a manageable and acceptable level through the use of these processes and controls. See the Risk Management Policy [BU 000-001B].

2.3. Sanctions Policy [164.308(a)(1)(ii)(C)] All workforce members, contractors, and agents of Boston University that have access to ePHI are expected to (i) fully comply with the policies developed to ensure compliance with HIPAA regulations and (ii) protect the privacy and security of ePHI. Boston University will maintain a formal documented process for applying appropriate sanctions against workforce members who do not comply with the security policies and procedures. At a minimum, the sanctions process will include:

2.3.1. Procedures for detecting and reporting workforce members' non-compliance with the security policies and procedures.

## **BOSTON UNIVERSITY**

2.3.2. Procedures for assessing the severity of the activities that are deemed non-compliant with the security policies and procedures.

2.3.3. Appropriate levels of sanctions relative to the severity of the violation.

2.3.4. Identification and documentation of the cause and rationale for issuing the sanction.

2.4. System Activity Review [164.308(a)(1)(ii)(D)] - Processes and procedures must be developed to facilitate the identification of potential security violations through the periodic review of audit logs, incident reports, access logs, and perimeter security logs. These reviews are primarily the responsibility of the Boston University Information Security group.

### **3. Boston University Security Responsibilities**

Boston University has identified several departments, committees, and teams whose primary aim is to protect the information resources of the CEs. This section describes each of these and their assigned function and responsibilities.

3.1. Information Services & Technology – The Boston University Information Security group coordinates the development and preparation of technical security standards. The technical standards use the following definitions:

- Requirements are rules that must be followed closely. Requirements use the words "will", "must" or "shall".

- Guidelines are rules that should be followed unless they are inappropriate or inordinately expensive to implement. Guidelines use the word "should".

The Boston University Information Security group is responsible for:

3.1.1. Assessing the adequacy of Boston University's protection measures, disaster recovery, and contingency planning for information resources.

3.1.2. Providing recommendations for improvements when they are needed.

3.1.3. Reviewing and recommending University technical security standards.

3.1.4. Ensuring effective implementation of approved security measures.

3.1.5. Coordinating Boston University awareness activities.

3.1.6. Coordinating physical security reviews for data processing computer sites and computer system support facility sites.

3.1.7. Coordinating Boston University security standards risk assessment.

3.1.8. Coordinating data security reviews of Boston University networks and systems.

## **BOSTON UNIVERSITY**

3.2. Covered Entity Management – Responsibilities of CE management, or their designated CE Security Official, include:

3.2.1. Implementing Boston University security policies, standards, and procedures.

3.2.2. Authorizing and managing access to information assets.

3.2.3. Allocating the necessary resources to comply with University security standards.

3.2.4. Promoting individual employee awareness of, and compliance with, University security standards.

3.2.5. Ensuring that an appropriate level of protection is provided for information resources, consistent with their criticality, value, and sensitivity.

3.2.6. Cooperating in the performance of periodic security self assessments and supporting formalized audit and risk assessment programs.

### **3.3. Systems Administrators**

3.3.1. Administer access to information systems and applications.

3.3.2. Configure systems to meet the security controls documented in Boston University Security Policy and Standards.

3.3.3. Administering system level security.

3.3.4. Immediately inform management of known or suspected compromises of sensitive information assets and violations of security policy, standards, and procedures and assist the Director, Boston University Information Security in security incident response efforts.

### **3.4. Users**

3.4.1. Comply with the Boston University HIPAA Privacy and Security policies, procedures, and standards.

3.4.2. Limit use of information assets to authorized purposes only.

3.4.3. Immediately inform management and Director, Boston University Information Security of known or suspected compromises of sensitive ePHI information assets or violations of information security policy, standards, and procedures.

## BOSTON UNIVERSITY

---

### Modification Control Sheet

| Rev | Date     | Author   | Description of Modification   |
|-----|----------|--|---|
| 0.0 | 20100429 | David Hutchings,<br>IS&T Information<br>Security | Changed all references to "University Information Systems" and "Information Systems and Technology" to "Information Services & Technology". |
|     |          |  |   |
|     |          |  |   |
|     |          |  |   |
|     |          |  |   |