1. Purpose - This policy addresses the general requirements of the Security Rule under the Health Insurance Portability and Accountability Act (HIPAA). Under the Security Rule, Boston University’s HIPAA-Covered Entities (CEs) are required to:

1.1. Ensure the confidentiality, integrity, and availability of all of the electronic protected health information (ePHI) the CEs create, receive, maintain, or transmit.

1.2. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.

1.3. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the HIPAA Privacy Rule.

1.4. Ensure compliance with the Security Rule by its workforce members.

2. Scope – This HIPAA Security Policy applies to all CEs. All CEs must maintain reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of their ePHI against any reasonably anticipated risks. The Security Rule also affects other departments such as the Office of Information Technology and Information Services & Technology. All workforce members of the CEs and affected workforce members of other departments must be aware of, and comply with, the security policies and procedures. Workforce members include administrators, faculty, staff, student trainees, independent contractors, volunteers, and others who may have access to ePHI in connection with their work, including research work. Any applicable contractual, legal or government regulatory requirements mandating more stringent requirements than are specified in this policy will supersede the requirements of this policy.
2.1. The CEs to which the HIPAA Security Rule applies include:

> HealthCare Providers:
  - The Danielsen Institute
  - School of Medicine Center for Human Genetics
  - Student Health Services
  - School of Dental Medicine Dental Clinic
  - Sargent College Rehabilitation Services
  - School of Dental Medicine Oral and Maxillofacial Pathology Laboratory
  - Faculty Staff Assistance Program

> Health Plans:
  - Boston University Dental Plan
  - Boston University Health Plan

In addition, the Boston University Occupational Health Center will comply with Security Rule policies and procedures.

3. HIPAA Security Rule - Overview

3.1. Guiding Principles: The HIPAA Security Rule is based on several important principles:

> Scalability: All sizes of CEs must be able to comply with the rule.

> Comprehensiveness: CEs must have a comprehensive security approach.

> Technology neutral: The rule does not require CEs to implement specific security technology (for example, a specific type of firewall or IDS). Each CE must have the appropriate technology to protect its ePHI.

> Internal and external security threats: CEs must protect their ePHI against both internal and external threats.

> Risk analysis: CEs must regularly conduct thorough and accurate risk analysis to assess the potential risks and vulnerabilities to ePHI.

3.2. Key Concepts: Key concepts of the Security Rule include:

> Standards-based: The rule requires CEs to comply with security standards. Step-by-step checklists are not provided.

> Reasonableness: CEs must take reasonable and appropriate measures to mitigate all reasonably-anticipated risks to their ePHI. In deciding what security measures to use, the CEs must take into account their resources and operational requirements, as well as the probability and criticality of risks to their ePHI.

> Full compliance: All members of a CE’s workforce, regardless of their work location (i.e., work remotely, or from home) must comply with the rule.
BOSTON UNIVERSITY

> Documentation: CEs must formally document a wide variety of security processes, policies, and procedures.

> Ongoing compliance: CEs must provide regular security training and awareness to its workforce, reassess its security measures periodically, and as needed, revise its security policies and procedures, under the direction of the HIPAA Security Officer.

3.3. Security Rule Requirements: The Security Rule’s requirements are organized into three categories: administrative safeguards, physical safeguards, and technical safeguards. There are 18 standards and numerous implementation specifications within these three categories. A standard defines what a CE must do. An implementation specification describes how it must be done. Implementation specifications are further divided into two types: required and addressable. Required specifications must be implemented. There are three alternatives for handling addressable implementation specifications:

> If a specific addressable implementation specification is determined to be reasonable and appropriate, the CE must implement it.

> If implementing a specific addressable implementation specification is not reasonable and appropriate, but the overall standard cannot be met without an additional security measure, a CE must:

  - Document why it would not be reasonable and appropriate to implement the implementation specification; and

  - Implement and document an equivalent alternative security measure.

> If implementing a specific addressable implementation specification is not reasonable and appropriate, but the overall standard can be met without implementation of an alternative security measure, a CE must document:

  - The decision not to implement the addressable specification;

  - Why it would not be reasonable and appropriate to implement the Implementation Specification; and

  - How the standard is being met.

4. HIPAA Security Policy: The CEs, under the direction of the HIPAA Security Officer, have implemented policies and procedures addressing the administrative, physical, and technical safeguards, as required. The security rule standards are listed here in this document with a reference to the policy document or documents that addresses each specific standard in detail.

4.1. Administrative Safeguards 164.308:

4.1.1.1. Risk Analysis: The initial and subsequent assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the CEs. See the Risk Analysis Policy [BU 000-001A].

4.1.1.2. Risk Management: Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. See the Risk Management Policy [BU 000-001B].

4.1.1.3. Sanction Policy: Appropriate sanctions against workforce members who fail to comply with the security policies and procedures.

4.1.1.4. Information System Activity Review: Procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

4.1.2. Assigned Security Responsibility: Boston University has designated Tracy A. Schroeder, Vice President for Information Services & Technology, as its HIPAA Security Officer. See the Assigned Security Responsibility Policy [BU 000-002].

4.1.3. Workforce Security: Policies and procedures to ensure that all members of the workforce have appropriate access to ePHI and to prevent those workforce members who do not have access to ePHI from obtaining access. See the Workforce Security Policy [BU 000-003].

4.1.3.1. Authorization and supervision: Procedures for the authorization and supervision of workforce members who work with ePHI or work in locations where it might be accessed.

4.1.3.2. Workforce Clearance: Procedures to determine that the access of a workforce member to ePHI is appropriate. See the Workforce Clearance Policy [BU 000-003A].

4.1.3.3. Termination: Procedures for terminating access to ePHI when the employment of a workforce member ends or otherwise as required.

4.1.4. Information Access Management: Policies and procedures for authorizing access to ePHI. See the Access Management Policy [BU 000-004] and the Policy Compliance Agreement Form [BU 000-004A].

4.1.4.1. Access Authorization: Policies and procedures for granting access to ePHI.

4.1.4.2. Access Establishment and Modification: Policies and procedures that establish, document, review, and modify a user’s right of access to ePHI.

4.1.5. Security Awareness and Training: IS&T has developed two web-based modules: (i) Security Awareness Presentation for Computer Users, and (ii) Workforce Training – HIPAA Security Rule. All workforce members who are subject to the Security Rule must complete the training, and all CEs must acknowledge to the HIPAA Security Officer that their workforce members have completed the training. See the Security Awareness and Training Policy [BU 000-005].
4.1.5.1. Security Reminders: The Awareness & Training Program includes periodic security reminders to update and reinforce the topics of training.

4.1.5.2. Protection from Malicious Software: End users can be valuable in the battle against malicious software (viruses, worms, Trojan Horses, spyware) if they are made aware of how to recognize, guard against, and report them. See the Protection from Malicious Software Policy [BU 000-005D].

4.1.5.3. Login Monitoring: Users should be trained to recognize unauthorized login attempts and made aware that their own logins to ePHI systems will be logged and audited.

4.1.5.4. Password Management: Since passwords are frequently the last line of defense protecting ePHI from unauthorized access, users should understand the importance of keeping their passwords private. Boston University CEs have a Password Policy. See the Password Policy [BU 000-005C]. All users should be made aware of and comply with this policy.

4.1.6. Security Incident Procedures: Policies and procedures to address security incidents. See the Security Incident Handling and Response Policy [BU 000-007].

4.1.6.1. Response and Reporting: Suspected or known security incidents shall be identified and an appropriate response shall be made. The known harmful effects of any security incident shall be mitigated, to the extent practicable. Security incidents and their outcomes shall be documented.

4.1.7. Contingency Plans: Policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. See the Disaster Recovery and Contingency Planning Policy [BU 000-006].

4.1.7.1. Data Backup Plans: Procedures to create and maintain retrievable copies of ePHI.

4.1.7.2. Disaster Recovery Plans: Procedures to restore any loss of data.

4.1.7.3. Emergency Mode Operation Plans: Procedures to enable continuation of critical processes for protection of the security of ePHI while operating in emergency mode.

4.1.7.4. Testing and Revision Procedures: Procedures for periodic testing and revision of contingency plans.

4.1.7.5. Applications and Data Criticality Analysis: Assessment of relative criticality of specific applications and data in support of other contingency plan components.

4.1.8. Evaluation: Periodic technical and non-technical evaluation of the security policies and procedures. See the Evaluation Policy [BU 000-009].

4.1.9. Business Associate Agreements and Other Arrangements: Written agreements and other arrangements that provide satisfactory assurances that each business associate will appropriately safeguard ePHI.
4.2. Physical Safeguards: 164.310.

4.2.1. Facility Access Controls: Policies and procedures to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. See the Facility Access Control Policy [BU 100-000].

4.2.1.1. Contingency Operations: Procedures that allow facility access in support of restoration of lost data under the disaster recovery plans and emergency mode operations plans in the event of an emergency.

4.2.1.2. Facility Security Plans: Policies and procedures to safeguard the facilities and equipment therein from unauthorized physical access, tampering, and theft.

4.2.1.3. Access Control and Validation Procedures: Procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

4.2.1.4. Maintenance Records: Policies and procedures to document repairs and modifications to the physical components of a facility which are related to security.

4.2.2. Workstation Use: Policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI. See the Workstation Use Policy [BU 100-001].

4.2.3. Workstation Security: Physical safeguards for all workstations that access ePHI to restrict access to authorized users. See the Workstation Security Policy [BU 100-002].

4.2.4. Device and Media Controls: Policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI in and out of a facility and the movement of these items within the facility. See the Device and Media Control Policy [BU 100-003].

4.2.4.1. Disposal: Policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

4.2.4.2. Media Re-Use: Procedures for removal of ePHI from electronic media before the media are made available for re-use.

4.2.4.3. Accountability: Records of the movements of hardware and electronic media and any person responsible for them.

4.2.4.4. Data Backup and Storage: Creation of a retrievable exact copy of ePHI when needed, before movement of equipment.

4.3. Technical Safeguards: 164.312
4.3.1. Access Control: Technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

4.3.1.1. Unique User Identification: Unique name and/or number for identifying and tracking user identity.

4.3.1.2. Emergency Access Procedures: Procedures for obtaining necessary ePHI during an emergency.

4.3.1.3. Automatic Logoff: Electronic procedures that terminate an electronic session after a predetermined time of inactivity.

4.3.1.4. Encryption and Decryption: Mechanisms to encrypt and decrypt ePHI.

4.3.2. Audit Controls: Hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use ePHI. CEs have enabled the logging functionality within applicable applications, operating systems, network traffic inspection devices, and the centralized access control tool eTrust Access Control. See the Security Management Policy [BU 000-001].

4.3.3. Integrity: Policies and procedures to protect ePHI from improper alteration or destruction. Access control policies and procedures for both Administrative and Physical safeguards ensure that data cannot be altered in an unauthorized fashion. Additional technical controls include error correcting memory (ECC RAM) and RAID disk storage technology described in Technical Security Standards documents for both UNIX and Windows servers.

4.3.3.1. Mechanism to Authenticate ePHI: Electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

4.3.4. Person or Entity Authentication: Procedures to verify that a person or entity seeking access to ePHI is the one claimed. The Information Access Management Policy [BU 000-004] dictates that access to ePHI and systems that store or process ePHI will require a valid user account and strong password compliant with the Password Policy [BU 000-005C].

4.3.5. Transmission Security: Technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

4.3.5.1. Integrity Controls: Security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

4.3.5.2. Encryption: Mechanism to encrypt ePHI whenever deemed appropriate.

5. Document Lifecycle [164.316(b)] - The HIPAA Security Officer, or designee, will periodically review this Policy Manual and supporting documentation and update them as needed to ensure the confidentiality, integrity, and availability of ePHI. Suggested modifications to these documents must be submitted in writing to Information Services & Technology for review. CEs must maintain all documentation (e.g., policies, procedures) required by the Security Rule for a period of six years from the date of creation or the date when it last was in effect, whichever is later.
later. This Policy Manual and supporting documentation are available to the workforce members to whom they apply and who are responsible for implementing the policies and procedures. See the Evaluation Policy [BU 000-009].