**Under the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act**

**Massachusetts General Laws chapter 93H and other laws**

## **RECITALS**

The purpose of this Agreement is to comply with the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act under the American Recovery and Reinvestment Act of 2009, (collectively “**HIPAA**”), as well as to comply with Massachusetts General Laws chapter 93H (the “**Massachusetts Security Breach Law**”), and other applicable data security laws, including in all cases the regulations, rules, orders, and guidelines promulgated with respect thereto, and all amendments and modifications thereto from time to time. References to HIPAA shall include, without limitation, the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Trustees of Boston University (the “University”) is a hybrid entity under HIPAA. The University has designated certain University health care providers as Covered Components (“Components”).

This Agreement is between the University and [\_\_\_\_\_\_\_\_\_\_\_\_], acting as the Business Associate of the University. This Agreement reflects both parties’ commitment to protect the privacy and security of Protected Health Information and to meet the data security, data breach notification, and other requirements of HIPAA, the Massachusetts Security Breach Law, and other applicable laws.

For valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows.

1. APPLICABILITY

University has retained Business Associate to perform the following services for or on behalf of one or more of its Components: [describe] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “Services”).

This Agreement concerns Protected Health Information (as defined in HIPAA), Personal Information (as defined in the Massachusetts Security Breach Law), and Other Confidential Information related to Business Associate’s performance of the Services for or on behalf of any of the Components, pursuant to any contracts and all amendments, renewals, replacements, and related contracts (“Contracts”) If, following execution of this Agreement, Business Associate provides additional services, or provides services to any of the Components, this Agreement will apply to those services as well.

Business Associate acknowledges that the obligations stated in this Business Associate Agreement are binding on Business Associate and its affiliates, subcontractors, employees, agents, and representatives.

**2. DEFINED TERMS**

All terms used herein, whether or not capitalized, shall be construed in accordance with HIPAA, the Massachusetts Security Breach Law, and other applicable laws as appropriate.

“Other Confidential Information” shall mean any and all (a) non-public information about the University, its schools, departments, units, related activities and operations, or property (tangible or intangible), (b) non-public or personal information of University patients/clients, personnel, students, alumni, affiliates, or contractors, (c) non-public information of third parties, and (d) any other information University specifically identifies as confidential.

## **3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.**

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information, Personal Information, and Other Confidential Information only as necessary to perform the Services or as Required by Law, provided that such use or disclosure would not cause either the University or Business Associate to violate HIPAA, the Massachusetts Security Breach Law, or other applicable law.

# **4. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.**

1. Business Associate agrees that it will comply with HIPAA, the Massachusetts Security Breach Law, and other applicable law, and will not take any action or refrain from taking any action that would cause the University to be in violation of such laws or that would violate those provisions of such laws directly applicable to Business Associate, except that Business Associate may use or disclose Protected Health Information, subject to the provisions of the following sentence (i) for Business Associate’s proper management and administration or (ii) to carry out the Business Association’s legal obligations. Notwithstanding the foregoing, if Business Associate discloses Protected Health Information for its proper management and administration or to carry out its legal responsibilities, it may do so only if the disclosure is required by law, or if Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information is breached, including, but not limited to, any unauthorized acquisition of, access to, use or disclosure of Protected Health Information. Business Associate agrees that it will ensure that its directors, officers, and employees comply with this Agreement.
2. Business Associate acknowledges that, as between Business Associate and the University, all Protected Health Information shall be and remain the sole property of the University, including any and all forms thereof developed by Business Associate in the course of its fulfillment of its obligations pursuant to the Agreement. Business Associate further represents that, to the extent Business Associate requests that University disclose Protected Health Information to Business Associate, such a request is only for the minimum necessary Protected Health Information for the accomplishment of Business Associate's purpose.
3. Business Associate agrees not to use or disclose Protected Health Information, Personal Information, or Other Confidential Information other than as permitted or required by this Agreement or as required by law. Business Associate shall use and disclose only the minimum Protected Health Information reasonably necessary to satisfy such obligations.
4. Business Associate agrees to use appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of Protected Health Information, Personal Information, and Other Confidential Information (including but not limited to complying with Subpart C of 45 CFR Part 164 with respect to electronic protected health information), to maintain and implement written policies and procedures addressing these safeguards, and to prevent any unauthorized use or disclosure thereof.
5. Business Associate agrees to ensure that any person or entity, including an agent, affiliate, or subcontractor, that creates, receives, maintains, or transmits Protected Health Information, Personal Information, and Other Confidential Information on behalf of Business Associate or to whom Business Associate provides such information agrees in writing to the same restrictions, conditions, and requirements that apply through this Agreement to Business Associate with respect to such information. Without limitation of the following, Business Associate agrees to ensure that any such affiliate, agent or subcontractor agrees to implement appropriate administrative, physical, and technical safeguards to protect it and to promptly report to Business Associate and the University any Breach of Protected Health Information or any security incident involving Protected Health Information, Personal Information, or Other Confidential Information.
6. If Business Associate has Protected Health Information in a Designated Record Set, Business Associate agrees to provide access, at the request of the University, and in the time and manner designated by the University, to Protected Health Information in the Designated Record Set, to the University or, as directed by the University, to an individual as necessary to satisfy the University’s obligations under 45 CFR 164.524 (Access of individuals to protected health information). If Business Associate has Protected Health Information in a Designated Record Set, Business Associate agrees to make any amendment(s) to Protected Health Information in the Designated Record Set that the University directs or agrees to pursuant to 45 CFR 164.526 (Amendment of protected health information), or take other measures as necessary to satisfy the University’s obligations under 45 CFR 164.526 as directed by the University. If Business Associate receives a request from an individual to access or amend Protected Health Information, Business Associate will promptly notify the University in writing of the details of such request.
7. Business Associate agrees to document all disclosures of Protected Health Information and information related to such disclosures in a manner sufficient to enable Business Associate and the University to comply with their obligations to respond to a request for an accounting of disclosures of Protected Health Information under 45 CFR 164.528 (Accounting of disclosures of protected health information) or other obligations under HIPAA. Business Associate agrees to provide sufficient information to the University or the appropriate individual, in a time and manner designated by the University, promptly upon request to enable the University to respond to a request for an accounting of disclosures of Protected Health Information or meet its other obligations under HIPAA. If Business Associate receives a request for an accounting of disclosures from an individual, Business Associate will promptly notify the University in writing of the details of such request.
8. To the extent Business Associate is to carry out one or more of the University’s obligations under Subpart E of 45 CFR Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to the University in the performance of such obligations.
9. Business Associate agrees to make its internal practices, books, records, policies, procedures, and other documentation relating to the use, disclosure, and protection of Protected Health Information available to the University, or at the request of the University to the Secretary of the Department of Health and Human Services or other federal agency with proper authority, in a time and manner designated by the University or the Secretary or other federal agency, for purposes of the Secretary or other federal agency determining the University’s or Business Associate’s compliance with HIPAA.
10. Business Associate agrees to maintain records relating to the use, disclosure, and protection of Protected Health Information, Personal Information, and Other Confidential Information for a minimum of six years.
11. Business Associate agrees to take such other action as may be required for compliance with HIPAA, the Massachusetts Security Breach Law, or other laws.

**5. OBLIGATIONS OF BUSINESS ASSOCIATE - SECURITY INCIDENT OR BREACH.**

* 1. Business Associate agrees to notify the University, verbally and by written notice, promptly upon discovering any security incident or suspected acquisition, access, use, modification, destruction or disclosure or Protected Health Information, Personal Information or Other Confidential Information not permitted under Subpart E of 45 CFR Part 164 or other laws, as applicable.
  2. Business Associate agrees to diligently investigate any security incident or suspected impermissible acquisition, access, use, modification, destruction, or disclosure of Protected Health Information, Personal Information, or Other Confidential Information.
  3. Business Associate agrees to promptly notify the University, verbally and by written notice, of any impermissible use or disclosure of the Protected Health Information, Personal Information or Other Confidential Information and any Breach of Unsecured Protected Health Information which it discovers. Notice of a Breach of Unsecured Protected Health Information shall be given promptly upon discovery in accordance with 45 CFR 164.410.
  4. Business Associate shall include in its notices to the University, to the extent possible (i) a description of what happened, including the date of the incident and the date of its discovery; (ii) the nature and extent of the Protected Health Information, Personal Information, or Other Confidential Information that were involved; including the types of identifiers and the likelihood of re-identification; (iii) the unauthorized person who used the information or to whom the disclosure was made; (iv) whether the information was actually acquired or viewed; (v) the extent to which the risk to the information has been mitigated; (vi) in the case of a breach, the identity of each individual whose Protected Health Information, Personal Information, or other personally identifiable information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed, and (vii) what Business Associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches. Business Associate agrees to provide the University with any other available information that may be required or requested.
  5. Business Associate agrees to take all necessary and reasonable steps to prevent any further unauthorized disclosure or use and to mitigate, to the extent practicable, any harmful effect of any unauthorized disclosure or use. Business Associate agrees to cooperate with and assist the University in any investigation, mitigation, prevention, and notification that the University may undertake as reasonably requested.
  6. Business Associate agrees to pay for reasonable costs to provide notifications required by HIPAA, when the breach is caused by Business Associate or occurs within Business Associate’s systems. If University agrees, Business Associate may send notifications required by HIPAA and approved by University.

**6. FURTHER COMPLIANCE WITH M.G. L. CH. 93H AND OTHER LAWS.**

1. General. Business Associate shall also comply and shall take all necessary and reasonable steps to assist the University to comply with all other applicable laws with respect to the information that Business Associate may access or hold.
2. Massachusetts Personal Information. To the extent that Business Associate holds Personal Information that is subject to the Massachusetts Security Breach Law, Business Associate shall implement a Comprehensive Written Information Security Plan as specified in 201 CMR 17.00 and provide a copy upon request. Business Associate agrees to allow the University to audit its processes and premises at any time, upon reasonable prior notice
3. Red Flags Rule. To the extent that Business Associate is a Service Provider of Covered Accounts as that term is defined by the Fair and Accurate Credit Transactions Act and the rules promulgated thereunder (the “Red Flags Rule”), Business Associate shall perform its activities under the Contracts in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft and shall promptly report to the University any incident which Business Associate detects as to Covered Accounts of the University.

**7. TERM AND TERMINATION.**

1. Term. This Agreement shall be effective as of the commencement of the contract or the functions, activities or services to which this Agreement applies. The provisions of this Agreement shall survive termination of any related contract between the parties, and shall terminate when all of the Protected Health Information, Personal Information, or Other Confidential Information provided by the University to Business Associate, or created or received by Business Associate on behalf of the University, is returned to the University, or destroyed at the University’s direction. If the parties mutually determine that it is infeasible for Business Associate to return or destroy Protected Health Information, Business Associate shall extend adequate protections to such information in accordance with the termination provisions of this Agreement.
2. Termination. The University, reserving all other rights and remedies, shall have the right to terminate this Agreement and any related contract between the parties in whole or in part, by giving written notice to Business Associate, if Business Associate has breached a material term of this Agreement and either has failed to cure the breach within the time period, if any, allowed by the University, or cure is not possible. In the event that neither cure nor termination is feasible (which shall be determined in the University’s sole discretion), Business Associate acknowledges and agrees that University has the right to report the breach to the Secretary, notwithstanding any other provision of the Agreement to the contrary.
3. Effect of Termination.
   1. Except as provided in subsection (ii) below, upon termination of this Agreement, for any reason, Business Associate shall return or, at the University’s direction, destroy all Protected Health Information, Personal Information, or Other Confidential Information received from the University, or created or received by Business Associate on behalf of the University. Business Associate shall retain no copies of the Protected Health Information, Personal Information, or Other Confidential Information except as may be permitted by law.
   2. In the event that Business Associate determines that returning or destroying the Protected Health Information, Personal Information, or Other Confidential Information is infeasible, Business Associate shall provide to the University written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of such information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information, Personal Information, or Other Confidential Information and limit further uses and disclosures thereof to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information, Personal Information, or Other Confidential Information.
   3. This section 7(c) shall apply to Protected Health Information, Personal Information, or Other Confidential Information that is in the possession of affiliates, subcontractors or agents of Business Associate. Business Associate agrees to recover, return and/or destroy any such information in the possession of its affiliates, subcontractors or agents. If the University agrees that it is infeasible to do so, Business Associate will require the affiliates, subcontractors or agents to agree to extend any and all protections of this Agreement to such information and to limit further uses and disclosures of such information to those purposes that make the return or destruction infeasible.

**8. MISCELLANEOUS.**

1. Integration with Related Contract. The provisions of this Agreement shall be and are hereby incorporated into any contract for Business Associate to provide the Services to the University now existing or subsequently established between the parties. The terms, agreements and obligations of the parties set forth herein shall be in addition to and shall supplement the terms, agreements and obligations of the parties in any related contract. In the event of any inconsistencies, the terms and conditions of this Agreement shall prevail, unless such related contract contains more stringent protections of Protected Health Information, Personal Information, or Other Confidential Information. No limitation of liability or damages in any related contract shall apply to this Agreement.
2. Amendment. This Agreement may only be amended or modified by written agreement of both parties. The parties agree to take such action to amend or supplement this Agreement as may be necessary for the University to comply with HIPAA, the Massachusetts Security Breach Law, and other applicable laws.
3. No Waiver. No provision of this Agreement that is required by law may be waived. No waiver of any other provision of this Agreement shall be effective unless given in writing signed by the party against whom the waiver is sought to be enforced. No failure to exercise, and no delay in exercising, any right, power, or privilege under this Agreement will operate as a waiver hereof, nor will any single or partial exercise of any right, power, or privilege under this Agreement preclude any further exercise of the same or any other right, power, or privilege hereunder.
4. Survival. The respective rights and obligations of the parties under this Agreement, including without limitation the obligations of Business Associate under section 5, shall survive termination of the Agreement to the extent necessary to fulfill their purposes.
5. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the University to comply with HIPAA, the Massachusetts Security Breach Law, and other applicable laws. If any part of this Agreement shall be adjudged by a court of competent jurisdiction to be invalid in any circumstance, such invalidity shall not affect any other provisions or circumstances.
6. Relationship of the Parties. Each of the parties is and shall perform its obligations under this Agreement as an independent contractor. Neither party has the authority to bind the other party.
7. Supersedes Prior BAA. This Agreement supersedes any prior Business Associate Agreement between the parties.

Signed and sealed by duly authorized representatives of the parties as of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_.

|  |  |
| --- | --- |
| TRUSTEES OF BOSTON UNIVERSITY | BUSINESS ASSOCIATE |
| On behalf of its Components  By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name:  Title: | By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name:  Title: |
| Contact Information for Notices:  BU HIPAA Privacy Officer  1 Silber Way Rm 909  Boston MA 02215  [hipaa@bu.edu](mailto:hipaa@bu.edu)  Contact Information for Notices Pursuant to  Section 5, Obligations of Business Associate –  Security Incident or Breach:  BU Information Security  930 Commonwealth Avenue  Boston, MA 02215  [irt@bu.edu](mailto:irt@bu.edu)  617-358-1100 | Contact Information for Notices:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |