

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (this "Agreement") effective as of _____, (the "Effective Date") by and between _____, a HIPAA-defined Covered Entity ("Covered Entity") and Northeastern University, through its Healthcare Systems Engineering Institute (the "University"), whose collaborative relationship with Covered Entity makes the University a HIPAA-defined Business Associate ("Business Associate") of the Covered Entity. Covered Entity and Business Associate are each a Party to this Agreement and are collectively the "Parties."

RECITALS:

A. The University has received a grant from the Centers for Medicare and Medicaid Services ("CMS") pursuant to which Covered Entity and Business Associate have agreed to work collaboratively on systems engineering and improvement projects pursuant to the grant, which collaboration may also include certain services by Business Associate to and on behalf of Covered Entity.

B. In the course of such collaboration, Business Associate may create, receive, use, maintain or disclose certain information on behalf of Covered Entity, some of which may constitute Protected Health Information or, in electronic form, Electronic Protected Health Information, (hereinafter singly or collectively referred to as "PHI") as defined by HIPAA.

C. The Parties intend to protect the privacy and provide for the security of PHI disclosed to Business Associate in compliance with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as the same may be amended from time to time, which include the Standards for the Privacy of Individually Identifiable Health Information (the "Privacy Regulations") (45 C.F.R. Parts 160 and 164) and the Security Standards for the Protection of Electronic PHI (the "Security Regulations") (45 C.F.R. Parts 160 and 164) (collectively, "HIPAA"), and the Health Information Technology for Economic and Clinical Health Act (Title XIII, Subtitle D) and its implementing regulations ("HITECH").

NOW, THEREFORE, for and in consideration of the mutual promises herein contained and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree as follows:

I. DEFINITIONS.

Capitalized terms used in this Agreement and not otherwise defined herein shall have that meaning given to them in HIPAA and HITECH.

II. GENERAL USE AND DISCLOSURE OF PHI BY BUSINESS ASSOCIATE.

A. Use or Disclosure to Provide Services. Business Associate may create, receive, use, maintain or disclose PHI as necessary pursuant to the collaboration described herein in accordance with HIPAA, HITECH, and this Agreement.

B. Use or Disclosure for Business Associate's Management and Administration and Legal Obligations. Notwithstanding any other provisions in this Agreement, Business Associate may use PHI for proper management and administration of Business Associate and to fulfill any present or future legal responsibilities of Business Associate provided that such uses are permitted under state and federal law. Business Associate may also disclose PHI to third parties for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate, provided that (a) the disclosures are required by law, or (b) Business Associate has received from the third party written assurances regarding confidential treatment of PHI, and that the third party will notify Business Associate of any instances of which it is aware in which confidentiality of the PHI has been breached, both as provided in C.F.R. §164.504(e).

C. De-Identification of PHI. Notwithstanding any other provisions in this Agreement, Business Associate may, in its discretion, de-identify any PHI received from or created or received on behalf of Covered Entity in

accordance with the de-identification standards set forth in the Privacy Regulations, and any such de-identified data shall not be deemed PHI for the purposes of this Agreement.

D. Use and Disclosure of Minimum Necessary PHI. Business Associate, when using, disclosing, or requesting PHI received from, or created or received by Business Associate on behalf of Covered Entity, must limit PHI to the Limited Data Set or, if needed, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

III. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.

A. Permitted Uses and Disclosures. Business Associate may not use or further disclose PHI received from, or created or received by Business Associate on behalf of, Covered Entity other than as permitted or required by this Agreement or as required by law.

B. Safeguards Against Misuse of Information. Business Associate must use appropriate safeguards to prevent use or disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity other than as provided for by this Agreement, as provided for in 45 C.F.R. § 164.504(e)(2).

C. Reporting Disclosures of PHI. Business Associate shall report to the Covered Entity any use or disclosure of PHI not provided for in this Agreement if it becomes aware of any such use or disclosure, as provided for in 45 C.F.R. § 164.504(e) (2). Business Associate agrees to have procedures in place for mitigating, to the extent practicable, any harmful effect known to Business Associate and arising from unauthorized uses or disclosures of PHI by Business Associate.

D. Agreements by Third Parties. Business Associate shall enter into an agreement with any agent or subcontractor to whom Business Associate provides PHI received from, or created or received by Business Associate on behalf of, Covered Entity pursuant to which such agent or contractor agrees to be bound by the same restrictions and conditions of this Agreement that apply to Business Associate with respect to such PHI, as provided for in 45 C.F.R. § 164.504(e)(2).

E. Access to Information. Business Associate shall provide access, at the request of Covered Entity or an Individual, to PHI maintained by Business Associate in a Designated Record Set(s), to Covered Entity, or as directed by Covered Entity, to an Individual in order to meet the requirements of 45 C.F.R. § 164.524.

F. Availability of PHI for Amendment. Business Associate shall make any amendment to PHI maintained in a Designated Record Set by Business Associate that is requested by Covered Entity, or as directed by Covered Entity, that is requested by an Individual in order to meet the requirements of 45 C.F.R. § 164.526.

G. Accounting of Disclosures. Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Business Associate shall provide to Covered Entity or, as directed by Covered Entity, to an Individual, information to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

H. Availability of Books and Records. Business Associate hereby agrees to make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of Health and Human Services (the "Secretary") for purposes of determining Covered Entity's compliance with HIPAA, as provided for in 45 C.F.R. § 164.504(e)(2). Notwithstanding the foregoing, nothing herein shall be deemed to require Business Associate to waive any attorney-client, accountant-client, or other legal privilege.

I. Security Obligations for PHI. Business Associate agrees that it will implement appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Regulations and 45 C.F.R. §164.314(a)(2).

J. Notification of Security Incident or Breach. If Business Associate becomes aware of any Security Incident, Business Associate shall report the incident to Covered Entity as provided for in 45 C.F.R. § 164.314(a)(2). Business Associate shall notify Covered Entity of a breach of Unsecured PHI without unreasonable delay and in no case later than 60 calendar days after discovery of the breach as required by 45 C.F.R. §164.410(b). For purposes of this Agreement, "Security Incident" shall not include activity such as "pings" and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as no such incident results in unauthorized access, use, or disclosure of electronic PHI.

K. Breach or Violation by Covered Entity. If Business Associate knows of a pattern of activity or practice that constitutes a material breach or violation of Covered Entity's obligations under this Agreement, Business Associate will notify Covered Entity in writing and will take reasonable steps to cure the breach or end the violation, if possible. If such steps are either not possible or are unsuccessful, the Business Associate upon written notice to Covered Entity will terminate its relationship with Covered Entity, if feasible; if termination is not feasible, Business Associate will report the breach or violation to the Secretary of Health and Human Services as required by 42 U.S.C. §17934(b).

IV. RESPONSIBILITIES OF COVERED ENTITY.

A. Requests for Uses or Disclosures. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would violate this Agreement, HIPAA, HITECH, or any applicable state or federal law.

B. Notice of Privacy Practices. Covered Entity hereby agrees to provide to Business Associate the notice of privacy practices (the "Notice") provided to Individuals (or their personal representatives) who are the subject of the PHI.

C. Written Permission. Covered Entity hereby agrees to ensure that it obtains Individuals' permission or the permission of Individuals' personal representatives, to the extent required under the Privacy Regulations and in the form required by the Privacy Regulations, for Business Associate's uses and disclosures of PHI contemplated by this Agreement or the collaboration described herein, and to inform Business Associate of any changes in, or withdrawal of, such written permission provided to Covered Entity by Individuals or their personal representatives, including without limitation revocations of authorizations pursuant to 45 C.F.R. §164.508. Covered Entity shall notify Business Associate of any restrictions to the use and disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restrictions affect Business Associate's use or disclosure of PHI.

V. TERMINATION.

A. Term. This Agreement shall begin on the Effective Date and will continue until termination or expiration of the collaboration described herein.

B. Termination for Cause. If Covered Entity makes the determination that Business Associate has breached a material term of this Agreement, Covered Entity may immediately terminate this Agreement. Covered Entity will provide Business Associate with written notice of the alleged breach and afford Business Associate an opportunity to cure said breach within thirty (30) calendar days after Business Associate's receipt of such notice.

C. Return or Destruction of PHI Upon Termination. Upon termination of this Agreement, Business Associate shall return or destroy all PHI received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form and retain no copies of such PHI. Notwithstanding the foregoing, to the extent that it is not feasible to return or destroy such PHI, Business Associate shall provide Covered Entity notification of the conditions that make return or destruction infeasible, and for all such data the terms and provisions of this Agreement shall survive the termination of the Agreement with respect to such PHI, and such PHI shall be used or disclosed solely for such purpose or purposes that made the return or destruction of the information infeasible.

VI. MISCELLANEOUS.

A. Amendments. The Parties agree to amend this Agreement if necessary to comply with privacy, security, or other applicable legal requirements. The Parties may modify, waive, or amend provisions of this Agreement only in a writing duly signed by authorized representatives of both Parties.

B. Survival. The respective rights and obligations of Business Associate and Covered Entity under Section V of this Agreement shall survive the termination of this Agreement.

C. References to Statutes or Regulations. References to a statutory or regulatory section shall be a reference to such section as it may be subsequently updated, amended, or modified.

The Parties have executed this Agreement as of the Effective Date.

Health System

Northeastern University
Healthcare Systems Engineering Institute

By:

By:

Print Name:

Print Name:

James C. Benneyan, PhD

Title:

Title:

Executive Director