BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION AND **<COMPANY/ORGANIZATION>**

Purpose. The purpose of this Business Associate Agreement (Agreement) is to establish requirements for the Department of Veterans Affairs (VA) Veterans Health Administration (VHA) and **<COMPANY/ORGANIZATION> <(government issued UEI#)>** in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules"), 45 C.F.R. Parts 160 and 164, for the Use and Disclosure of Protected Health Information (PHI) under the terms and conditions specified below.

With respect solely to the subject matter herein, the terms and conditions in this National Business Associate Agreement supersede any previously executed National Business Associate Agreement, as well as any local Business Associate Agreement between **<COMPANY/ORGANIZATION>** and a component of VHA. Accordingly, this National Business Associate Agreement, unless otherwise provided, will control and cannot be superseded, modified, or nullified by any local Business Associate Agreement or Data Use Agreement.

Scope. As described in this Agreement and any other applicable contracts or agreements, **<COMPANY/ORGANIZATION>** will provide **the following** services to, for, or on behalf of VHA:

- **Services**
- **Services**

In order for **<COMPANY/ORGANIZATION>** to provide such services, VHA will provide PHI to **<COMPANY/ORGANIZATION>**, and

<COMPANY/ORGANIZATION> will use or disclose PHI in accordance with this Agreement.

Definitions. Unless otherwise provided, the following terms used in this Agreement have the same meaning as defined by the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, PHI, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured PHI, and Use.

"Breach" shall have the same meaning as described at 45 C.F.R. § 164.402. For the purposes of this Agreement, Breach shall refer to an acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Rules or by this Agreement.

"Business Associate" shall have the same meaning as described at 45 C.F.R. § 160.103. For the purposes of this Agreement, Business Associate shall refer to **<COMPANY/ORGANIZATION>**, including its employees, officers, or any other

agents that create, receive, maintain, or transmit PHI as described below.

"Covered Entity" shall have the same meaning as the term is defined at 45 C.F.R. § 160.103. For the purposes of this Agreement, Covered Entity shall refer to **VHA**.

"Incident" shall have the same meaning as described in VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, which is an event that has resulted in, or had the potential to result in, unauthorized access to or disclosure of VA sensitive personal information in a manner not permitted under the applicable confidentiality provisions. An incident that involves access or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless Business Associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment using at least the listed factors in the Breach Notification Rule.

"Protected Health Information" or "PHI" shall have the same meaning as described at 45 C.F.R. § 160.103. "Protected Health Information" and "PHI" as used in this Agreement include "Electronic Protected Health Information" and "EPHI." For the purposes of this Agreement and unless otherwise provided, the term shall also refer to PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity or receives from Covered Entity or from another Business Associate of Covered Entity.

"Sensitive Personal Information" or "SPI," is a subset of "VA Sensitive Data" and shall have the same meaning as described in 38 U.S.C § 5727, any information about an individual maintained by VA, including education, financial transaction, medical history, and criminal or employment history; information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. SPI, which includes PHI, is VA Sensitive Data, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

"Subcontractor" shall have the same meaning as the term is defined at 45 C.F.R. § 160.103. For the purposes of this Agreement, Subcontractor shall refer to a contractor of any person or entity, other than Covered Entity or Business Associate, that creates, receives, maintains, or transmits PHI under the terms of this Agreement.

Terms and Conditions. Covered Entity and Business Associate agree as follows:

1. Ownership of PHI. PHI is and remains data owned by Covered Entity as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of

whether a compliant Business Associate Agreement is in place.

2. Use and Disclosure of PHI by Business Associate. Unless otherwise provided, Business Associate:

A. May not use or disclose PHI other than as permitted or required by this Agreement and in compliance with VHA Directive 1605.01, Privacy and Release of Information, or may not use or disclose PHI in a manner that would violate the HIPAA Privacy Rule if done by Covered Entity, except that it may use or disclose PHI:

(1) To perform the functions and services for Covered Entity described above in "Scope";
(2) As required by law or to carry out its legal responsibilities;
(2) For the proper management and administration of Business Associate; or
(3) To provide Data Aggregation services relating to the health care operations of Covered Entity.

B. Must use or disclose PHI in a manner that complies with Covered Entity's minimum necessary policies and procedures as provided in VHA Directive 1605.02, Minimum Necessary Standard.

C. May de-identify PHI created or received by Business Associate under this Agreement, provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule and that such de-identified information is used solely for purposes of providing or improving Business Associate's services for Covered Entity or for another lawful purpose approved in advance and in writing by Covered Entity. Business Associate shall not sell or market de-identified data sets created from PHI.

3. Obligations of Business Associate. In connection with any Use or Disclosure of PHI, Business Associate must:

A. Business Associate must comply with all VA and VHA privacy policies including but not limited to VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information; VHA Directive 1605, VHA Privacy Program; VHA Directive 1605.01, Privacy and Release of Information; VHA Directive 1605.02, Minimum Necessary Standard; 1605.03 Privacy Compliance and Accountability Program; and 1605.05, Business Associate Agreements.

B. Consult with Covered Entity before using or disclosing PHI whenever Business Associate is uncertain whether the Use or Disclosure is authorized under this Agreement.

C. Implement appropriate administrative, physical, and technical safeguards and controls to protect PHI and document applicable policies and procedures to

prevent any Use or Disclosure of PHI other than as provided by this Agreement.

D. Provide satisfactory assurances that PHI created or received by Business Associate under this Agreement is protected in accordance with this Agreement and applicable law to the greatest extent feasible.

E. Notify Covered Entity no later than by midnight following the next business day after Business Associate's discovery (as described in (1) below) of any incident, such as an actual or suspected access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of this Agreement "that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of VA information or a VA information system" accessible by VA users "or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies," per the Federal Information Security Management Act, 44 USC 3501-3518. The parties acknowledge and agree that this section does not apply to incidents that are trivial and do not result in unauthorized access, use, or disclosure of PHI that is Electronic Protected Health Information, including without limitation pings and other broadcast attacks on **<COMPANY ORGANIZATION>** firewall, port scans, unsuccessful log-on attempts, and denials of service attacks, or other failed attempts does not need to be reported and no additional notice to VHA shall be required.

(1) For purposes of this notification, an incident as described above will be treated as discovered by Business Associate when such event is known to any employee, officer, or other agent (other than the individual who committed the incident) of Business Associate or, by exercising reasonable diligence, would have been known to an employee, officer, or other agent of Business Associate.

(2) Notification to Covered Entity shall be to the VHA Information Access and Privacy Office, by email to VHABAAIssues@va.gov.

(3) Absent Covered Entity's request or approval, and unless otherwise required by law, Business Associate shall not directly notify individuals or the Department of Health and Human Services of incidents involving PHI created or received by Business Associate as an agent of Covered Entity.

F. Provide a written report to Covered Entity of any actual or suspected access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of this Agreement, including any Incident or Breach of PHI, within ten (10) business days of the initial notification to the Covered Entity.

(1) The written report of an incident as described above will document the following to the extent reasonably known:

(a) The identity of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, disclosed, modified, or destroyed;

(b) A description of what occurred, including the date of the incident and the date of the discovery of the incident (if known);

(c) A description of the types of secured or unsecured PHI that was involved;

(d) A description of what is being done to investigate the incident, to mitigate further harm to individuals, and to protect against future Security Incidents; and

(e) Any other information as required by 45 C.F.R. §§ 164.404(c) and 164.410.

(2) The written report shall be directed to:

VHA Information Access and Privacy Office
Department of Veterans Affairs – Veterans Health Administration
Digital Health Office (DHO)
Office of Health Informatics (10DH03A)
810 Vermont Avenue NW
Washington, DC 20420

and submitted by email at VHABAAIssues@va.gov

G. To the greatest extent feasible, mitigate any harm due to a Use or Disclosure of PHI by Business Associate in violation of this Agreement that is known or, by exercising reasonable diligence, should have been known to Business Associate.

H. To the extent feasible, use only agents and Subcontractors that are physically located within a jurisdiction subject to the laws of the United States or its Territories in connection with the services provided to Covered Entity and PHI of Covered Entity. Business Associate must notify Covered Entity if any agent or subcontractors performing services under this agreement are physically located outside a jurisdiction subject to the law of the United States or its territories.

I. Enter into Business Associate Agreements with contractors and Subcontractors as appropriate under the HIPAA Rules and this Agreement. In doing so Business Associate:

(1) Must ensure that the terms of any agreement between Business Associate and a contractor or Subcontractor are at least as restrictive as Business Associate Agreement between Business Associate and Covered Entity.

(2) Must ensure that contractors and Subcontractors agree to the same restrictions and conditions that apply to Business Associate and obtain satisfactory written assurances from them that they agree to those restrictions and conditions.

(3) Unless approved by Covered Entity in advance and in writing, may not amend any terms of such Agreement, in any way to make them inconsistent with the obligations of Business Associate or any contractors or Subcontractors in connection with or in consideration of the HIPAA Rules or this Agreement.

J. Within five (5) business days of a written request from Covered Entity:

(1) Make available information for Covered Entity to respond to an individual's request for access to PHI about him/her.

(2) Make available information for Covered Entity to respond to an individual's request for amendment of PHI about him/her and, as determined by and under the direction of Covered Entity, incorporate any amendment to the PHI.

(3) Make available PHI for Covered Entity to respond to an individual's request for an accounting of Disclosures of PHI about him/her.

K. Unless required by law the Business Associate shall not take any action in response to an individual's request for access, amendment, or accounting and shall direct the individual to contact the VHA Privacy Office at 1-877-461-5038.

L. To the extent Business Associate is required to carry out Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the provisions that apply to Covered Entity in the performance of such obligations.

M. Provide to the Secretary of Health and Human Services and to Covered Entity records related to Use or Disclosure of PHI, including its policies, procedures, and practices, for the purpose of determining Covered Entity's, Business Associate's, or a Subcontractor's compliance with the HIPAA Rules.

N. Upon completion or termination of the applicable contract(s) or agreement(s), return or destroy all PHI and other VA data created or received by Business Associate during the performance of the contract(s) or agreement(s). No such information will be retained by Business Associate unless retention is required by law or specifically permitted by Covered Entity. If return or destruction is not feasible, Business Associate shall continue to protect the PHI in accordance with the HIPAA Rules or this Agreement and use or disclose the information under this Agreement only for the purpose of making the return or destruction feasible, as

required by law, or as specifically permitted by Covered Entity. Business Associate shall provide written assurance that either all PHI has been returned or destroyed, or any information retained will be safeguarded and used and disclosed only as permitted under this paragraph.

O. Be liable to Covered Entity for civil or criminal penalties imposed on Covered Entity, in accordance with 45 C.F.R. §§ 160.402(c) and 160.410, and with the HITECH Act, 42 U.S.C. §§ 17931(b), 17934(c), for any violation of the HIPAA Rules or this Agreement due to any action or inaction by Business Associate.

P. Upon written request, Business Associate will make available to the VHA Privacy Compliance and Accountability Office (PCA), access to all physical operations, policies, procedures, and personnel, pertaining to the Business Associate's obligations to the Covered Entity for implementing a HIPAA-compliant privacy and security program upon request within a reasonable timeframe not to exceed twenty (20) business days of the request. VHA would bear the cost of the PCA audit team.

4. Obligations of Covered Entity. Covered Entity agrees that it:

A. Will not request Business Associate to make any Use or Disclosure of PHI in a manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if made by Covered Entity, except as permitted under Section 2 of this Agreement.

B. Will promptly notify Business Associate in writing of any restrictions on Covered Entity's authority to use or disclose PHI that may limit Business Associate's Use or Disclosure of PHI or otherwise affect its ability to fulfill its obligations under this Agreement.

C. Has obtained or will obtain from Individuals any authorization necessary for Business Associate to fulfill its obligations under this Agreement.

D. Will promptly notify Business Associate in writing of any change in Covered Entity's Notice of Privacy Practices, or any modification or revocation of an Individual's authorization to use or disclose PHI, if such change or revocation may limit Business Associate's Use and Disclosure of PHI or otherwise affect its ability to perform its obligations under this Agreement.

5. Amendment. Business Associate and Covered Entity agree to enter into good faith negotiations to amend this Agreement, as necessary, for Covered Entity and Business Associate to comply with the requirements of the HIPAA Rules or other applicable law.

6. Termination.

A. Automatic Termination. This Agreement will automatically terminate upon completion of Business Associate's duties under all underlying Agreements or by termination of such underlying Agreements.

B. Termination Upon Review. This Agreement may be terminated by Covered Entity upon review as provided by Section 9 of this Agreement.

C. Termination for Cause. In the event of a material breach of this Agreement by Business Associate, Covered Entity:

(1) Will provide Business Associate written notice of the material breach and an opportunity for Business Associate to cure the breach or end the violation within the reasonable time specified by Covered Entity, such period being no less than 30 calendar days, and;

(2) May terminate this Agreement if Business Associate does not cure the breach or end the violation within the reasonable time specified by Covered Entity.

D. Effect of Termination. Termination of this Agreement will result in cessation of activities by Business Associate involving PHI under this Agreement.

E. Survival. The obligations of Business Associate under Section 3 above shall survive the termination of this Agreement as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate Agreement is in place.

7. No Third-Party Beneficiaries. Nothing expressed or implied in this Agreement confers any rights, remedies, obligations, or liabilities whatsoever upon any person or entity other than Covered Entity and Business Associate, including their respective successors or assigns.

8. Other Applicable Law. This Agreement does not abrogate any responsibilities of the parties under any other applicable law.

9. Review Date. The provisions of this Agreement will be reviewed by Covered Entity and Business Associate every two (2) years from Effective Date to determine the applicability and accuracy of the Agreement based on the circumstances that exist at the time of review. Business Associate will provide an appropriate point of contact to VHABAAIssues@va.gov who will work with VHA to accomplish this review.

10. Effective Date. This Agreement shall be effective on the last signature date below.

Department of Veterans Affairs	**<Company/Organization?>**
Veterans Health Administration	
By:	**By:**
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**