

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION AND

Whereas, (Business Associate) provides services to the Department of Veterans Affairs Veterans Health Administration (Covered Entity); and

Whereas, in order for Business Associate to provide services to Covered Entity, Covered Entity discloses to Business Associate Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996), and its implementing regulations, 45 C.F.R. Parts 160, 162, and 164 ("the HIPAA Privacy and Security Rules"); and

Whereas, the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115 (2009), pursuant to Title XIII of Division A and Title IV of Division B, called the Health Information Technology for Economic and Clinical Health (HITECH) Act, provides modifications to the HIPAA Privacy and Security Rules; and

Whereas, Department of Veterans Affairs Veterans Health Administration is a "Covered Entity" as that term is defined in the HIPAA implementing regulations, 45 C.F.R. § 160.103; and

Whereas, , including its employees, officers, contractors, subcontractors, or any other agents, as a recipient of PHI from Covered Entity in order to provide services to Covered Entity, is a "Business Associate" of Covered Entity as the term "Business Associate" is defined in the HIPAA implementing regulations, 45 CFR 160.103; and

Whereas, pursuant to the Privacy and Security Rules, all Business Associates of Covered Entities must agree in writing to certain mandatory provisions regarding the Use and Disclosure of PHI; and

Whereas, the purpose of this Agreement is to comply with the requirements of the Privacy and Security Rules, including, but not limited to, the Business Associate Agreement requirements at 45 C.F.R. §§ 164.308(b), 164.314(a), 164.410, 164.502(e), and 164.504(e), as may be amended.

NOW, THEREFORE, the Covered Entity and Business Associate agree as follows:

1. Definitions. Unless otherwise provided in this Agreement, capitalized terms and phrases that are defined in the Privacy and Security Rules have the same meanings as set forth in the Privacy and Security Rules. When the phrase "Protected Health Information" and the abbreviation "PHI" are used in this 2. Ownership of PHI. PHI provided by Covered Entity to Business Associate and its agents and subcontractors, or gathered by them on behalf of the Covered Entity, under this BAA are the property of Covered Entity. Agreement, they include the phrase "Electronic Protected Health Information" and the abbreviation "EPHI."

2. Ownership of PHI. PHI provided by Covered Entity to Business Associate and its contractors, subcontractors, or other agents, or gathered by them on behalf of Covered Entity under this Agreement is the property of Covered Entity.

3. Scope of Use and Disclosure by Business Associate of Protected Health Information. Unless otherwise limited herein, Business Associate may:

A. Make Uses and Disclosures of PHI that is disclosed to it by Covered Entity or received by Business Associate on behalf of Covered Entity as necessary to perform its obligations under this Agreement and all applicable agreements, provided that such Use or Disclosure would not violate the HIPAA Privacy Rule if made by Covered Entity and complies with Covered Entity's minimum necessary policies and procedures;

B. Use the PHI received in its capacity as a Business Associate of Covered Entity for its proper management and administration and to fulfill any legal responsibilities of Business Associate;

C. Make a Disclosure of the PHI in its possession to a third party for the proper management and administration of Business Associate or to fulfill any legal responsibilities of Business Associate; provided, however, that the Disclosure would not violate the HIPAA Privacy Rule if made by Covered Entity, or is Required by Law; and Business Associate has received from the third party written assurances that (a) the information will be held confidentially and used or further disclosed only for the purposes for which it was disclosed to the third party or as Required By Law, (b) the third party will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the information may have been breached, and (c) the third party has agreed to implement reasonable and appropriate steps to safeguard the information;

D. Engage in Data Aggregation activities, consistent with the HIPAA Privacy Rule; and

E. De-identify any and all PHI created or received by Business Associate under this Agreement, provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule.

4. Obligations of Business Associate. In connection with its Use or Disclosure of PHI, Business Associate agrees that it will:

A. Consult with Covered Entity before making the Use or Disclosure whenever Business Associate is uncertain whether it may make a particular Use or Disclosure of PHI in performance of this Agreement;

B. Ensure any employee, officer, contractor, subcontractor, or other agent of Business Associate who has access to PHI receives at a minimum annual privacy and security awareness training that conforms to the requirements of Covered Entity;

C. Develop and document policies and procedures and use reasonable and appropriate safeguards to prevent use or disclosure of PHI other than as provided by this Agreement;

D. To the extent practicable, mitigate any harmful effect of 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;

E. Maintain a system or process to account for any Security Incident, Privacy Incident, or Use or Disclosure of PHI not authorized by this Agreement of which Business Associate becomes aware;

F. Notify Covered Entity within 24 hours of Business Associate's discovery of any incident which may potentially be a data breach, including a HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI, whether secured (PHI which has been destroyed or in the alternative has been rendered unreadable, unusable, or undecipherable through methodology specified by the Department of Health and Human Services in guidance issued under § 13402(h)(2) of the HITECH Act) or unsecured (PHI not secured through the use of a technology which renders it unusable, unreadable, or indecipherable through such methodology), not provided for by this Agreement and promptly provide a report to Covered Entity within ten (10) business days of the notification;

(1) An incident is any physical, technical, or personal activity or event that, a reasonable person believes, increases risk of inappropriate or unauthorized use or disclosure of PHI or causes Covered Entity to be considered non-compliant with the HIPAA Privacy and Security Rules;

(2) A breach, as defined in 45 C.F.R. § 164.402, is an unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the individual;

(3) A breach, consistent with 45 C.F.R. § 164.410(a)(2), will be treated as discovered as of the first day on which such breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate, or any employee, officer, contractor, subcontractor, or other agent of Business Associate;

(4) Notification will be made by Business Associate to the Director, Health Information Governance, by email at VHABAAIssues@va.gov of any HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI not provided for by this Agreement; and

(5) A written report of the incident, submitted to the Director, Health Information Governance, within ten (10) business days after initial notification, will document the following:

(a) The identification of each individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the breach;

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

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

(d) A description of what is being done to investigate the breach, to mitigate further harm to individuals, and the reasonable and appropriate safeguards being taken to protect against future breaches; and

(e) Any other information described in 45 C.F.R. § 164.404(c)

(6) This report should be documented as a letter and sent to:

Director, Health Information Governance
Department of Veterans Affairs – Veterans Health Administration
Office of Informatics and Analytics (10P)
810 Vermont Avenue NW
Washington, DC 20420

G. Implement administrative, physical, and technical safeguards and controls for the PHI that Business Associate receives, maintains, or transmits on behalf of Covered Entity, including policies, procedures, training, and sanctions, in compliance with Federal Information Security Management Act (FISMA), Pub. L. No. 107-347, 116 Stat. 2946 (2002); the HIPAA Privacy and Security Rules, 45 C.F.R. Parts 160, 162, and 164; standards and guidance from the Office of Management and Budget and the National Institute of Standards and Technology; Federal Records Act requirements, National Archives and Records Administration regulations, to include applicable records retention schedules, and other laws, regulations, and policies pertaining to safeguarding VA Sensitive Data;

H. Require contractors, subcontractors, or other agents to whom Business Associate provides PHI received from Covered Entity to agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement, including implementation of administrative, physical, and technical safeguards and controls, including policies, procedures, training, and sanctions, in compliance with the above-referenced legal authorities;

I. Obtain satisfactory written assurances from contractors, subcontractors, or other agents to whom Business Associate provides PHI received from Covered Entity that the contractors, subcontractors, or other agents agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement;

J. If Business Associate maintains PHI in a Designated Record Set or Privacy Act System of Records, within ten (10) business days of receiving a written request from Covered Entity:

(1) Make available PHI in the Designated Record Set or System of Records necessary for Covered Entity to respond to individuals' requests for access to PHI about them that is not in the possession of Covered Entity;

(2) Incorporate any amendments or corrections to the PHI in the Designated Record Set or System of Records in accordance with the Privacy Act and the HIPAA Privacy Rule; and

(3) Maintain the information necessary to document the disclosures of PHI sufficient to make an accounting of those disclosures as required under the Privacy Act, 5 U.S.C. § 552a, and the HIPAA Privacy

Rule, and within ten (10) business days of receiving a request from Covered Entity, make available the information necessary for Covered Entity to make an accounting of Disclosures of PHI about an individual in the Designated Record Set or System of Records;

K. Utilize only contractors, subcontractors, or other agents who are physically located within a jurisdiction subject to the laws of the United States and ensure that no contractor, subcontractor, or agent maintains, processes, uses, or discloses PHI received from Covered Entity in any way that will remove the PHI from such jurisdiction. Any modification to this provision must be approved by Covered Entity in advance and in writing;

L. Provide satisfactory assurances that the confidentiality, integrity, and availability of the PHI provided by Covered Entity under this Agreement are reasonably and appropriately protected;

M. Upon completion or termination of the applicable contract(s) or agreement(s), return and/or destroy, at Covered Entity's option, the PHI gathered, created, received, or processed during the performance of the contract(s) or agreement(s). No data will be retained by Business Associate, or contractor, subcontractor, or other agent of Business Associate, unless retention is required by law and specifically permitted by Covered Entity. As deemed appropriate by and under the direction of Covered Entity, Business Associate shall provide written assurance that all PHI has been returned to Covered Entity or destroyed by Business Associate. If immediate return or destruction of all data is not possible, Business Associate shall notify Covered Entity and assure that all PHI retained will be safeguarded to prevent unauthorized Uses or Disclosures;

N. Be liable to Covered Entity for any civil or criminal penalties imposed on Covered Entity under the HIPAA Privacy and Security Rules in the event of a violation of the Rules as a result of any practice, behavior, or conduct by Business Associate;

O. Make available to Covered Entity its practices, policies and procedures, for the purpose of determining compliance with this Agreement and underlying agreements; and

P. Make available to the Secretary of Health and Human Services Business Associate's internal practices, books, and records, including policies and procedures, relating to the Use or Disclosure of PHI for purposes of determining Covered Entity's compliance with the Privacy and Security Rules, subject to any applicable legal privileges.

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

A. Has obtained or will obtain from Individuals any consents, authorizations, and other permissions necessary or required by laws applicable to Covered Entity for Business Associate and Covered Entity to fulfill their obligations under this Agreement;

B. Will promptly notify Business Associate in writing of any restrictions on the Use and Disclosure of PHI about Individuals that Covered Entity has agreed to that may affect Business Associate's ability to perform its obligations under this Agreement; and

C. Will promptly notify Business Associate in writing of any change in, or revocation of, permission by an Individual to use or disclose PHI, if such change or revocation may affect Business Associate's ability to perform its obligations under this Agreement;

6. Material Breach and Termination.

A. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

- (1) Provide an opportunity for Business Associate to cure the breach or end the violation;
- (2) Terminate this Agreement and underlying contract(s) if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or
- (3) Immediately terminate this Agreement and underlying contract(s) if cure is not possible; or
- (4) If Business Associate has breached a material term of this Agreement and neither termination nor cure is feasible, report the violation to the Secretary of Health and Human Services.

B. Termination Upon Review. This Agreement may be terminated by Covered Entity, if appropriate, upon review as defined in Section 12 of this Agreement.

C. Automatic Termination. This Agreement will automatically terminate upon completion of the Business Associate's duties under all underlying agreements or by mutual written agreement to terminate underlying agreements.

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

7. Amendment. Business Associate and Covered Entity agree to take such action as is necessary to amend this Agreement for Covered Entity to comply with the requirements of the Privacy and Security Rules or other applicable law.

8. No Third Party Beneficiaries. Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

9. Other Applicable Law. This Agreement does not and is not intended to abrogate any responsibilities of the parties under any other applicable law.

10. Effect of Agreement. With respect solely to the subject matter herein, the terms and conditions in a National Business Associate Agreement, executed by the Director, Health Information Governance, or a designated representative, will supersede any local business associate agreement between Business Associate and a component of VHA. The parties also agree that a National Business Associate Agreement, unless itself modified by the parties, will control and cannot be superseded, modified, or nullified by any local business associate agreement.

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

12. Review Date. The provisions of this Agreement will be reviewed by Covered Entity every two years from Effective Date to determine the applicability of the agreement based on the relationship of the parties at the time of review.

**Department of Veterans Affairs
Veterans Health Administration**

By: _____
Name: _____
Title: _____
Date: _____

By: _____
Name: _____
Title: _____
Date: _____