

BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT (the “BAA”) is made and entered into as of [DATE] by and between:

Covered Entity: [COVERED ENTITY NAME], a Corporation
 (“Covered Entity”)

Business Associate: VIGIL HEALTH SOLUTIONS, INC., a Corporation (“Vigil” or “Business Associate”, in accordance with the meaning given to those terms at 45 CFR § 164.501). In this BAA, Covered Entity and Business Associate are each a “Party” and, collectively, are the “Parties”.

This BAA is an Attachment to the Master Supply and Services Agreement (“MSA”) by and between Business Associate and Covered Entity, dated _____. In the event of any inconsistency between the terms of this BAA and the MSA, the terms of this BAA will control.

BACKGROUND

- I. Covered Entity is either a “covered entity” or “business associate” of a covered entity as each are defined under the Health Insurance Portability and Accountability Act of 1986, Public Law 104-191, as amended by the HITECH ACT (as defined below) and the related regulations promulgated by HHS (as defined below) (collectively, “HIPAA”) and, as such, is required to comply with HIPAA’s provisions regarding the confidentiality and privacy of Protected Health Information (as defined below);
- II. The Parties have entered into or will enter into one or more agreements under which Vigil provides or will provide certain specified services to Covered Entity (collectively, the “Agreement”);
- III. In providing services pursuant to the Agreement, Vigil may have access to Protected Health Information;
- IV. By providing the services pursuant to the Agreement, Vigil will become a “business associate” of the Covered Entity as such term is defined under HIPAA;
- V. Both Parties are committed to complying with all federal and state laws governing confidentiality and privacy of health information, including, but not limited to, the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Part 160 and Part 164, Subparts A and E (collectively, the “Privacy Rule”); and
- VI. Both Parties intend to protect the privacy and provide for the security of Protected Health Information disclosed to Vigil pursuant to this Agreement, HIPAA and other applicable laws.

AGREEMENT

NOW, THEREFORE, in consideration of the mutual and conditions contained herein and the continued provision of PHI by Covered Entity to Vigil under the Agreement in reliance on this BAA, the Parties agree as follows:

1. **Definitions.** For the purposes of this BAA, the Parties give the following meaning to each of the terms in this Section 1 below. Any capitalized term used in this BAA, but otherwise defined, has the meaning given to that term in the Privacy Rule or pertinent law.
 - A. **"Affiliate"** means a subsidiary or affiliate of Covered Entity that is, or has been, considered a covered entity, as defined by HIPAA.
 - B. **"Breach"** means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI, as defined in 45 CFR § 164.402.
 - C. **"Breach Notification Rule"** means the portion of HIPAA set forth in Subpart D of 45 CFR Part 164.
 - D. **"Data Aggregation"** means, with respect to PHI created or received by Vigil in its capacity as the "business associate" under HIPAA of Covered Entity, the combining of such PHI by Vigil with the PHI received by Vigil in its capacity as a business associate of one or more other "covered entity" under HIPAA, to permit data analyses that relate to the Health Care Operations (defined below) of the respective covered entities. The meaning of "data aggregation" in this BAA shall be consistent with the meaning given to that term in the Privacy Rule.
 - E. **"Designated Record Set"** has the meaning given to such term under the Privacy Rule including 45 CFR § 164.501.B.
 - F. **"De-Identify"** means to alter the PHI such that the resulting information meets the requirements described in 45 CFR §§164.514(a) and (b).
 - G. **"Electronic PHI"** means any PHI maintained in or transmitted by electronic media as defined in 45 CFR § 160.103
 - H. **"Health Care Operations"** has the meaning given to that term in 45 CFR § 164.501.
 - I. **"HHS"** means the U.S. Department of Health and Human Services.
 - J. **"HITECH Act"** means the Health Information Technology for Economic and Clinical Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.
 - K. **"Individual"** has the same meaning given to that term in 45 CFR §§164.501 and 160.130 and includes a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
 - L. **"Privacy Rule"** means that portion of HIPAA set forth in 45 CFR Part 160 and Part 164, Subparts A and E.
 - M. **"Protected Health Information"** or **"PHI"** has the meaning given to the term "protected health information" in 45 CFR §§164.501 and 160.103, limited to the information created or received by Vigil from or on behalf of the Covered Entity.

- N. “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- O. “Security Rule” means the Security Standards for the Protection of Electronic Health Information provided in 45 CFR Part 160 & Part 164, Subparts A and C.
- P. “Unsecured Protected Health Information” or “Unsecured PHI” means any “protected health information” as defined in 45 CFR §§164.501 and 160.103 that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary in the guidance issued pursuant to the HITECH Act and codified at 42 USC § 17932(h).

2. Use and Disclosure of PHI.

- A. Except as otherwise provided in this BAA, Vigil may use or disclose PHI as reasonably to provide the services described in the Agreement to Covered Entity, and to undertake other activities of Vigil permitted or required of Vigil by this BAA or as required by law.
- B. Except as otherwise limited by this BAA or federal or state law, Covered Entity authorizes Vigil to use the PHI in its possession for the proper management and administration of Vigil’s business and to carry out its legal responsibilities. Vigil may disclose PHI for its proper management and administration, provided that (i) the disclosures are by law; or (ii) Vigil obtains, in writing, prior to making any disclosure to a third party (a) reasonable assurances from this third party that the PHI will be held confidential as provided under this BAA and used or further disclosed only as required by law or for the purpose for which it was disclosed to this third party and (b) an agreement from this third party to notify Vigil immediately of any breaches of the confidentiality of the PHI, to the extent it has knowledge of the breach.
- C. Vigil will not use or disclose PHI in a manner other than as provided in this BAA, as permitted under the Privacy Rule, or as required by law. Vigil will use or disclose PHI, to the extent practicable, as a limited data set or limited to the minimum necessary amount of PHI to carry out the intended purpose of the use or disclosure, in accordance with Section 13405(b) of the HITECH ACT (codified as 42 USC § 17935(b)) and any of the act’s implementing regulations adopted by HHS, for each use or disclosure of PHI.
- D. Upon request, Vigil will make available to Covered Entity any of Covered Entity’s PHI that Business Associate or any of its agents or subcontractors have in their possession.
- E. Vigil may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

- 3. Safeguards Against Misuse of PHI. Vigil will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided by the Agreement or this BAA and Vigil agrees to implement administrative, physical, and technical

safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Vigil agrees to take reasonable steps, including providing adequate training to its employees to ensure compliance with this BAA and to ensure that the actions or omissions of its employees or agents do not cause Vigil to breach the terms of this BAA.

4. **Reporting Disclosures of PHI and Security Incidents.** Vigil will report to Covered Entity in writing any use or disclosure of PHI not provided for by this BAA of which it becomes aware and Vigil agrees to report to Covered Entity any Security Incident affecting Electronic PHI of Covered Entity of which it becomes aware. Vigil agrees to report any such event within 30 business days. Vigil reserves the right to conduct audit(s) and investigation(s) into a suspected Security Incident of which it becomes aware; if such audit(s) and investigation(s) reveal that no PHI was compromised, then Vigil will have no duty to notify or reimburse Covered Entity.

Reporting Breaches of Unsecured PHI. Vigil will notify Covered Entity in writing promptly upon the discovery of any Breach of Unsecured PHI in accordance with the requirements set forth in 45 CFR § 164.410, but in no case later than 30 calendar days after the discovery of a Breach. Vigil will reimburse Covered Entity for any costs incurred by it in complying with the requirements of Subpart D of 45 CFR §164 that are imposed on Covered Entity as a result of a Breach committed by Vigil.

5. **Mitigation of Disclosures of PHI.** Vigil will take reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to VIGILVIGIL of any use or disclosure of PHI by Vigil or its agents or subcontractors in violation of the requirements of this BAA.
6. **Agreements with Agents or Subcontractors.** Vigil will ensure that any of its agents or subcontractors that have access to, or to which Vigil provides PHI, agree in writing to the restriction and conditions concerning uses and disclosures of PHI contained in this BAA and agree to implement reasonable and appropriate safeguards to protect any Electronic PHI that it creates, received, maintains or transmits on behalf of Vigil or, through the Vigil, Covered Entity. Vigil shall ensure that all subcontracts and agreements provide the same level of privacy and security as this BAA.

7. **Access to PHI by Individuals.**

- A. Upon request, Vigil agrees to furnish Covered Entity with copies of the PHI maintained by Vigil in a Designated Record Set in the time and manner designated by Covered Entity to enable Covered Entity to respond to an Individual's request for access to PHI under 45 CFR §164.524.
- B. In the event any Individual or personal representative requests access to the Individual's PHI directly from Vigil, Vigil within 10 business days, will

forward that request to Covered Entity. Any disclosure of, or decision not to disclose, the PHI requested by an Individual or a personal representative and compliance with the requirements applicable to an Individual's right to obtain access to PHI shall be the sole responsibility of Covered Entity.

8. Amendment of PHI.

- A.** Upon request and instruction from Covered Entity, Vigil will amend PHI or a record about an Individual in a Designated Record Set that is maintained by, or otherwise within the possession of, Vigil as directed by Covered Entity in accordance with procedures established by 45 CFR §164.526. Any request by Covered Entity to amend such information will be completed by Vigil within 15 business days of Covered Entity's request.
- B.** In the event that any Individual requests that Vigil amend such Individual's PHI or record in a Designated Record Set, Vigil within 10 business days will forward this request to Covered Entity. Any amendment of, or decision not to amend, the PHI or record as requested by an Individual and compliance with the requirements applicable to an Individual's right to request an amendment of PHI will be the sole responsibility of Covered Entity.

9. Accounting of Disclosures.

- A.** Vigil will document any disclosures of PHI made by it to account for such disclosures as required by 45 CFR §164.528(a). Vigil also will make available information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosures in accordance with 45 CFR §164.528. At a minimum, Vigil will furnish Covered Entity the following with respect to any covered disclosures by Vigil: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI, and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure which includes the basis for such disclosure.
- B.** Vigil will furnish to Covered Entity information collected in accordance with this Section 10, within 10 business days after written request by Covered Entity, to permit Covered Entity to make an accounting of disclosures as required by 45 CFR §164.528, or in the event that Covered Entity elects to provide an Individual with a list of its business associates, Vigil will provide an accounting of its disclosures of PHI upon request if the Individual, if and to the extent that such accounting is required under the HITECH ACT or under HHS regulations adopted in connection with the HITECH ACT.
- C.** In the event an Individual delivers the initial request for an accounting directly to Vigil, Vigil will within 10 business days forward such request to Covered Entity.

10. Availability of Books and Records. Vigil will make available its internal practices, books, agreements, records, and policies and procedures relating to

the use and disclosure of PHI, upon request, to the Secretary of HHS for purposes of determining Covered Entity's and Vigil's compliance with HIPAA, and this BAA.

11. Responsibilities of Covered Entity. With regard to the use and/or disclosure of Protected Health Information by Vigil, Covered Entity agrees to:

- A.** Notify Vigil of any limitation(s) in its notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect Vigil's use or disclosure of PHI.
- B.** Notify Vigil of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Vigil's use or disclosure of PHI.
- C.** Notify Vigil of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Vigil's use or disclosure of PHI.
- D.** Except for data aggregation or management and administrative activities of Vigil, Covered Entity shall not request Vigil to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

12. Term and Termination.

- A.** This BAA will become effective on the date first written above and will continue in effect until all obligations of the Parties have been met under the Agreement and under this BAA.
- B.** Covered Entity may terminate this BAA, the Agreement, and any other related agreements if Vigil has breached a material term of this BAA and Vigil has failed to cure that material breach within 30 days after written notice from Covered Entity. Covered Entity may report the problem to the Secretary of HHS if termination is not feasible.
- C.** If Vigil determines that Covered Entity has breached a material term of this BAA, then Vigil will provide Covered Entity with written notice of the existence of the breach and shall provide Covered Entity with 30 days to cure the breach. Covered Entity's failure to cure the breach within the 30-day period will be grounds for immediate termination of the Agreement and this BAA by Vigil. Vigil may report the breach to the HHS.
- D.** Upon termination of the Agreement or this BAA for any reason, all PHI maintained by Vigil will be returned to Covered Entity or destroyed by Vigil. Vigil will not retain any copies of such information. This provision will apply to PHI in the possession of Vigil's agents and subcontractors. If return or destruction of the PHI is not feasible, in Vigil's reasonable judgment, Vigil will furnish Covered Entity with notification, in writing, of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of the PHI is infeasible, Vigil will extend the protections of this BAA to such information for as long as Vigil retains such information and will limit further uses and disclosures

to those purposes that make the return or destruction of the information not feasible. The Parties understand that this Section 14.D. will survive any termination of this BAA.

13. Effect of BAA.

- A. This BAA is a part of and subject to the terms of the Agreement, except that to the extent any terms of this BAA conflict with any term of the Agreement, the terms of this BAA will govern.
- B. Except as expressly stated in this BA or as provided by law, this BAA will not create any rights in favor of any third party.

14. Regulatory References. A reference in this BAA to a section in HIPAA means the section as in effect or as amended at the time.

15. Notices. All notices, requests and demands or other communications to be given under this BAA to a Party will be made via either first class mail, registered or certified or express courier, or electronic mail to the Party's address given below:

- A. If to Covered Entity, to: [COVERED ENTITY'S NAME]
[MAILING ADDRESS]
[ATTN.]
[TELEPHONE]
[E-MAIL]
- B. If to Vigil, to: Vigil
[MAILING ADDRESS]
[ATTN.]
[TELEPHONE]
[E-MAIL]

16. Amendments and Waiver. This BAA may not be modified, nor will any provision be waived or amended, except in writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

17. HITECH ACT Compliance. The Parties acknowledge that the HITECH Act includes significant changes to the Privacy Rule and the Security Rule. The privacy subtitle of the HITECH Act sets forth provisions that significantly change the requirements for business associates and the agreements between business associates and covered entities under HIPAA and these changes may be further clarified in forthcoming regulations and guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued with respect to the HITECH Act. The Parties also agree to negotiate in good faith to modify this BAA as reasonably necessary to comply with the HITECH Act and its regulations as they become effective but, in the event that the Parties are unable to reach an agreement on such a modification, either

Party will have the right to terminate this BAA upon 30 days' prior written notice to the other Party.

In light of the mutual agreement and understanding described above, the Parties execute this BAA as of the date first written above.

Covered Entity: _____ **Date:** _____

Print Name: _____

Title: _____

Business Associate: _____ **Date:** _____

Print Name: _____

Title: _____