



SUB-BUSINESS ASSOCIATE AGREEMENT PROTECTED HEALTH INFORMATION

THIS SUB-BUSINESS ASSOCIATE AGREEMENT (this “Agreement”), dated as of the date set forth below, by and between _____, the “Business Associate” (“Business Associate”) and OpenVPN, Inc. (“Sub-Business Associate”), with reference to the following facts:

The Business Associate is providing services to an entity (a “Covered Entity”) that involves the collection, processing, storage, and creation of Protected Healthcare Information (as defined below). The Business Associate and Sub-Business Associate have entered into an agreement (a “Services Agreement”) pursuant to which Sub-Business Associates is providing goods or services to the Business Associate, which services may include the collection, processing, storage, and/or creation of that Protected Health Care Information.

The Business Associate and Sub-Business Associate are entering into this Agreement for the purpose of complying with the Health Insurance Portability and Accountability Act of 1996 and the Final Rule for Standards for Privacy of Individually Identifiable Health Information adopted by the United States Department of Health and Human Services and codified at 45 C.F.R. part 160 and part 164, subparts A & E (the “Privacy Rule”), the HIPAA Security Rule (the “Security Rule”), codified at 45 C.F.R. Part 164 Subpart C, and Subtitle D of the Health Information Technology for Economic and Clinical Health Act (“HITECH”), including C.F.R. Sections 164.308, 164.310, 164.312, 164.316, and 164.402, as amended, including relevant state regulations (collectively hereinafter “HIPAA”) with respect to Protected Healthcare Information the Sub-Business Associate may collect, process, store, or create in the course of performing services or for providing goods to the Business Associate under the Services Agreement.

NOW THEREFORE, in consideration of the mutual covenants, promises, and agreements contained herein, the parties hereto agree as follows:

1. **DEFINITIONS.** For the purposes of this Agreement, capitalized terms shall have the meanings ascribed to them below. All capitalized terms used but not otherwise defined herein will have the meaning ascribed to them by HIPAA.

- a. “Individual” means the natural person to whom the Protected Health Information pertains.
- b. “Protected Health Information” or “PHI” is any information, whether oral or recorded in any form or medium that is created, received, maintained, or transmitted by Sub-Business Associate, from or on behalf of Business Associate, that identifies an individual or might reasonably be used to identify an individual and relates to: (i) the individual’s past, present or future physical or mental health; (ii) the provision of health care to the individual; or (iii) the past, present or future payment for health care.
- c. “Secretary” shall refer to the Secretary of the U.S. Department of Health and Human Services.

d. “Unsecured PHI” shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. This definition applies to both hard copy PHI and electronic PHI.

2. OBLIGATIONS OF SUB-BUSINESS ASSOCIATE

a. Confidentiality

(i) Sub-Business Associate shall use or disclose PHI only in connection with performing its obligations under this Agreement and the Service Agreement and not in any other manner other than as permitted by this Agreement or permitted or required by law.

(ii) Sub-Business Associate may disclose PHI as is reasonably necessary to perform its obligations under this Agreement and the Services Agreement. Sub-Business Associate may also disclose PHI in connection with the proper management and administration of Sub-Business Associate’s business, but only if:

A. That disclosure is required by law, or

B. Sub-Business Associate obtains reasonable assurances from the person or entity to whom the information is disclosed that the information remain confidential and be used or further disclosed only as required by law and only for the purpose for which it was disclosed to the person or entity, and the person or entity notifies the Sub-Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

b. Safeguards. Sub-Business Associate shall employ appropriate administrative, technical, and physical safeguards, consistent with the size and complexity of Sub-Business Associate’s operations, to protect the confidentiality, integrity, and availability of PHI and to prevent the use or disclosure of PHI in any manner inconsistent with this Agreement. Sub-Business Associate shall comply, where applicable, with the Security Rule with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for in this Agreement. Sub-Business Associate agrees to ensure that any agent or subcontractor to whom it provides electronic PHI agrees to implement reasonable and appropriate safeguards to protect such information.

c. Disclosure of PHI for Remuneration

(i) Sub-Business Associate shall not directly or indirectly receive remuneration in exchange for disclosing PHI without the prior written consent of Business Associate. The restrictions in the previous sentence do apply to disclosures of PHI by Sub-Business Associate:

A. For public health purposes pursuant to 45 C.F.R. § 164.512(b) or § 164.514(e);

B. for research purposes pursuant to 45 C.F.R. § 164.512(i) or § 164.514(e), where the only remuneration received by Subcontractor is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;

C. for treatment, payment or Health Care Operations purposes pursuant to 45 C.F.R. § 164.506(a);

D. to or by Sub-Business Associate for activities that Sub-Business Associate undertakes on behalf of Business Associate pursuant to 45 C.F.R. §§ 164.502(e) and 164.504(e), and the only remuneration provided is by Business Associate to Sub-Business Associate for the performance of such activities;

E. to an Individual, or to Business Associate on behalf of the Individual, when requested under 45 C.F.R. §§ 164.524, 164.526 or 164.528; and

F. that are required by Law, subject to the requirements of 45 C.F.R. § 164.512(a).

(ii) Sub-Business Associate shall not use or disclose PHI for marketing purposes, as defined in 45 C.F.R. § 164.501, except as specifically authorized by Business Associate in writing.

d. Availability of Books and Records. Sub-Business Associate shall permit the Secretary and other regulatory and accreditation authorities to audit Sub-Business Associate's internal practices, books, records, policies, and procedures at reasonable times as they pertain to the use and disclosure of PHI received from, or created or received by Sub-Business Associate on behalf of, Business Associate and/or Covered Entity for the purpose of verifying that Covered Entity is in compliance with the requirements of HIPAA.

e. Access to and Amendment of PHI. Upon written request by Business Associate, to the extent Business Associate demonstrates that it is incapable of doing so itself, Sub-Business Associate shall make PHI in a Designated Record Set available to Business Associate for inspection and copying to enable Business Associate's Covered Entity or Business Associate customers to fulfill their obligations under the Privacy Rule, including without limitation 45 C.F.R. §§ 164.524 and 164.526. No later than twenty (20) calendar days following a request by Business Associate (unless a longer response time is authorized by Business Associate in writing), Sub-Business Associate shall:

(i) Produce the PHI in the form and format requested by Business Associate if the information is readily producible in such form or format; or, if not, then (i) in another computerized format (e.g., MS Word or Excel, text, HTML or PDF); or (ii) if Sub-Business Associate does not maintain the information electronically, then in readable hard copy form or another form and format as agreed by Business Associate and Sub-Business Associate;

(ii) transmit a copy of PHI to another person or entity as directed by Business Associate or its Covered Entity or Business Associate partners on behalf of the Individual; and

(iii) incorporate any amendments to PHI as directed by Business Associate.

Business Associate shall pay Sub-Business Associate a reasonable fee and reimburse Sub-Business Associate for its out of pocket costs incurred in complying with the Business Associate's request made under this Section 2e.

f. Accounting of Disclosures

(i) Sub-Business Associate agrees to document disclosures of PHI, if any, and information related to such disclosures as required by and in accordance with 45 C.F.R. § 164.528.

(ii) No later than 20 days following a written request by Business Associate (unless a longer response time is authorized by Business Associate in writing), Sub-Business Associate shall provide an accounting of disclosures of PHI pertaining to the Individual(s) subject of the request, to enable Business Associate's Covered Entity or Business Associate partners to fulfill their obligations under 45 C.F.R. § 164.528. The accounting shall include the details specified in 45 C.F.R. § 164.528(b)(2).

(iii) If and to the extent Sub-Business Associate uses or maintains an electronic health record ("EHR"), with respect to PHI, Sub-Business Associate shall, in addition to the requirements set forth in paragraphs (a) and (b) above, track and provide accounting of disclosures of EHR for purposes of treatment, payment or Health Care Operations of Business Associate's Covered Entity or Business Associate partners, as provided in 45 C.F.R. § 164.506.

(iv) Sub-Business Associate agrees to maintain an accounting of disclosures described in paragraph f(i) for a period of six (6) years after termination of this Agreement, and disclosures described in paragraph f(iii) for a period of three (3) years after termination of this Agreement.

g. Reporting Obligations - Breach Notification. Sub-Business Associate shall report to Business Associate in writing any use or disclosure of PHI of which it becomes aware that is not in accordance with this Agreement or the Privacy Rule, including Breaches of Unsecured PHI, as required by 45 C.F.R. § 164.410, and any Security Incidents, without unreasonable delay and in no case later than thirty (30) calendar days after the discovery of any such use, disclosure, Breach, or Security Incident. Upon discovery of a Breach or Security Incident, Sub-Business Associate will undertake a documented risk assessment in accordance with the Breach Response Rule to determine whether the acquisition, access, use or disclosure of the PHI at issue is likely to compromise the affected PHI. Sub-Business Associate shall make this determination in coordination and consultation with Business Associate. Sub-Business Associate shall make and retain records of such determinations, including the basis for any determination that an unauthorized use or disclosure of PHI is not a Breach that requires notification of affected individuals, regulators and others, and shall provide the documents supporting such determination to Business Associate if requested. Sub-Business Associate's determination that the Breach is likely to result in low probability of compromise of the affected PHI is subject to review and approval by Business Associate. If Business Associate disagrees with Sub-Business Associate's determination of low probability of compromise, Sub-Business Associate shall comply with Business Associate's determination and comply with the requirements of this Agreement consistent with such determination. Sub-Business Associate shall mitigate, to the extent commercially practicable, any harmful effect known to Sub-Business Associate arising from a use or disclosure of PHI by Sub-Business Associate in violation of the requirements of this Agreement (including a Breach of Unsecured PHI) a Security Incident; however, nothing in this Section will impose an obligation on Sub-Business Associate to notify the Covered Entity or Individual in question directly of such Breach, Security Incident, or other disclosure, and the Business Associate undertakes to provide such notice to that Covered Entity or Individual as required by law.

h. Subcontractors and Agents. Sub-Business Associate may disclose PHI to a subcontractor of Sub-Business Associate and may allow such subcontractor to create, receive, maintain or transmit PHI on Sub-Business Associate's behalf if that subcontractor enters into a contract with Sub-Business Associate whereby that subcontractor is bound by the same restrictions and conditions that apply to Sub-Business Associate with respect to the PHI. If Sub-Business Associate becomes aware of a violation the Rules by the subcontractor or a pattern of activity or practice of that subcontractor that constitutes a material breach or violation of the subcontractor's obligation under the contract with Sub-Business Associate, Sub-Business Associate will take reasonable steps to cure that breach or end that violation, as applicable, and, if such steps are unsuccessful, terminate the contract or arrangement to the extent reasonably feasible.

i. Return of PHI. During the term of this Agreement, when any particular PHI is no longer necessary for the performance of the services to Business Associate or for any other purposes for which Sub-Business Associate is authorized to use or disclose the PHI, upon written request from Business Associate, Sub-Business Associate shall without unreasonable delay return or, if Business Associate gives written permission, securely destroy such PHI in whatever form or medium and retain no copies of such PHI. In the event that Sub-Business Associate determines that returning or destroying the PHI is infeasible, Sub-Business Associate shall provide to Business Associate notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of the PHI is infeasible, Sub-Business Associate shall extend the protections of this Agreement (and of any additional requirements imposed by HIPAA, HITECH or the Rules) to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Sub-Business Associate maintains such PHI.

3. **OBLIGATIONS OF BUSINESS ASSOCIATE**

a. Permissible Requests

(i) Business Associate shall not request Sub-Business Associate to use or disclose PHI in any manner that would violate applicable federal or state laws if such use or disclosure were made by Business Associate, Covered Entity, or any contractor of Business Associate or Covered Entity.

(ii) Business Associate may request Sub-Business Associate to disclose PHI directly to another party only for the purposes allowed by HIPAA, the HITECH Act and the Rules.

(iii) Business Associate shall use its best efforts to minimize the disclosure of PHI to Sub-Business Associate where the disclosure of that information is not needed for Subcontractor to provide or services to Business Associate.

b. Notifications

(i) Business Associate shall notify Sub-Business Associate of any limitation in any applicable notice of privacy practices in accordance with 45 CFR Section 164.520, to the extent that such limitation may affect Sub-Business Associate's use or disclosure of PHI.

(ii) Business Associate shall notify Sub-Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Sub-Business Associate's use or disclosure of PHI.

(iii) Business Associate shall notify Sub-Business Associate of any restriction to the use or disclosure of PHI that Business Associate has agreed to in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect Sub-Business Associate's use or disclosure of PHI. Sub-Business Associate agrees to comply, upon communication by Business Associate, with any restrictions to the use or disclosure of PHI that Business Associate has agreed to in accordance with 45 CFR Section 164.522.

4. **TERM AND TERMINATION**

a. General Term and Termination. This Agreement shall become effective on the date of this Agreement and shall terminate upon the termination or expiration of the Service Agreement.

b. Material Breach

(i) Where either party has knowledge of a material breach by the other party and cure is possible, the non-breaching party shall provide the breaching party with an opportunity to cure. Where said breach is not cured to the reasonable satisfaction of the non-breaching party within five (5) business days of the breaching party's receipt of notice from the non-breaching party of said breach, the non-breaching party shall, if feasible, terminate this Agreement and the portion(s) of the Service Agreement affected by the breach.

(ii) Where either party has knowledge of a material breach by the other party and cure is not possible, the non-breaching party shall, if feasible, terminate this Agreement and the portion(s) of the Service Agreement affected by the breach.

(iii) Notwithstanding the foregoing, upon Business Associate's acknowledgement of a material breach of this Agreement by the Sub-Business Associate, Business Associate and/or Covered Entity is authorized to terminate this Agreement and the Service Agreement if breach remains uncured or mitigated.

c. Return or Destruction of PHI. Upon termination of this Agreement for any reason, Sub-Business Associate shall:

(i) Return to Business Associate or destroy all PHI that Sub-Business Associate or any of its subcontractors and agents still maintain in any form, and Sub-Business Associate shall retain no copies of such information; or

(ii) If Sub-Business Associate determines, and reasonably can show, that such return or destruction is not feasible, and Business Associate agrees, Sub-Business Associate shall extend the protections of this Agreement to such information and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible, in which case Sub-Business Associate's obligations under this Section shall survive the termination of this Agreement.

d. Survival. The rights and obligations of Sub-Business Associate under this Agreement will survive the termination of this Agreement.

5. **MISCELLANEOUS**

- a. Amendment. If any of the regulations promulgated under HIPAA or the HITECH Act are amended or interpreted in a manner that renders this Agreement inconsistent therewith, the parties shall amend this Agreement to the extent necessary to comply with such amendments or interpretations.
- b. Interpretation. Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA and the HITECH Act.
- c. No Third-Party Beneficiaries. This Agreement is intended for the benefit of Sub-Business Associate and Business Associate only. Nothing is intended to confer or create, nor be interpreted to confer or create, any rights, remedies, obligations or liabilities to or for any third-party beneficiary under this Agreement.
- d. Limitation on Liability – Exclusion of Damages. In no event will the liability of Sub-Business Associate for breach of this Agreement exceed the total payments made by Business Associate to Sub-Business Associate for products or services unless such breach arises out of the intentional misconduct or gross negligence of Sub-Business Associate. NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES FOR ANY CLAIM ARISING OUT OF THIS AGREEMENT (REGARDLESS OF WHETHER SUCH CLAIM IS FOR BREACH OF CONTRACT, TORT, OR VIOLATION OF LAW) EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- e. Independent Contractor. The parties acknowledge Sub-Business Associate is an independent contractor of Business Associate. Nothing in this Agreement creates a partnership, joint venture, or principal-agent relationship between the parties.
- f. Interpretation. Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA and the HITECH Act.
- g. Conflicting Terms – Application. This Agreement pertains solely to the parties' rights and obligations with respect to PHI and does not affect any rights or obligations of the parties with respect to data that is not PHI or any other transaction or subject matter set forth in the Services Agreement. If the terms of this Agreement conflict with any terms of the Service Agreement as they pertain to PHI, the terms of this Agreement shall govern and control.
- h. Notices. Any notices pertaining to this Agreement shall be given in writing and shall be directed to a party at the address and to the attention of the person appearing below that party's signature to this Agreement or to such other address or person as that party provides by notice to the other party. Notices may be delivered personally, by recognized overnight courier (such as Federal Express) with delivery charges paid by the sender, by certified mail, return receipt requested, or by e-mail with acknowledgment of receipt given by the intended recipient or proof of delivery obtained by the sender. Notices will be deemed given and received upon delivery if delivered personally or by e-mail, one (1) business day after deposit with the overnight courier, or four (4) business days after deposit with the postal service.
- i. Severability. The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of

this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

[REMAINDER OF PAGE LEFT BLANK INTENTIONALLY.
SIGNATURES APPEAR ON FOLLOWING PAGE.]

IN WITNESS WHEREOF, each of the undersigned has duly executed this Agreement on behalf of the party and on the date set forth below.

SUB-BUSINESS ASSOCIATE

BUSINESS ASSOCIATE

OPENVPN, INC.

[NAME OF BUSINESS ASSOCIATE]

By: _____

By: _____

Title: _____

Title: _____

Signed: _____

Signed: _____

E-Mail: _____

E-Mail: _____