

BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

This Business Associate Subcontractor Agreement (“**BAA**”) is entered into between **CLIENT** (as defined in the above) and **VENDOR** (as defined in the above). **CLIENT** and **VENDOR** expressly agree to be bound by the terms of this BAA for any and all products or services provided by **VENDOR** to **CLIENT** under the agreement(s) between the Parties.

WHEREAS, **CLIENT** is a Party to agreements pursuant to which **CLIENT** provides services to healthcare organizations (“**HCOs**”). **CLIENT** and **VENDOR** are Parties to the Agreement pursuant to which **VENDOR** provides services, as defined in the Agreement, to **CLIENT**, and in connection with the provision of the services, certain **HCOs** Protected Health Information (“**PHI**” as defined in 45 C.F.R. §164.501) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”) may be disclosed to **VENDOR**;

WHEREAS, **HCO(s)** are “Covered Entities” as that term is defined in the **HIPAA** implementing regulations, 45 C.F.R. Part 160 and Part 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“the Privacy Rule”); and 45 C.F.R. Part 164, Subpart C, the Security Standards for the Protection of Electronic Protected Health Information (“the Security Rule”);

WHEREAS, **CLIENT**, as a recipient of **PHI** from **HCO(s)** is a “Business Associate” as that term is defined in the Privacy Rule and the Security Rule;

WHEREAS, as used herein, the Privacy Rule and the Security Rule are each deemed to include the amendments thereto that are included in the Modifications to the **HIPAA** Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the **HIPAA** Rules; Final Rule (the “Omnibus Rule”), 78 Fed. Reg. 5565;

WHEREAS, pursuant to the Privacy Rule and the Security Rule, all Business Associates of Covered Entities must agree in writing to certain mandatory provisions regarding the Use and Disclosure of **PHI**, including a provision requiring contractors or agents to whom the Business Associate provides **PHI** to agree to the same conditions and restrictions that apply to the Business Associate;

WHEREAS, the Health Information Technology for Economic and Clinical Health Act (“**HITECH**”) adopted as part of the American Recovery and Reinvestment Act of 2009 imposes certain requirements on Business Associates with respect to privacy, security and breach notification and contemplates that such requirements shall be implemented by regulations (such statutory and regulatory provisions may be referred to collectively as the “**HITECH** BA Provisions”);

WHEREAS, the purpose of this BAA is to comply with the Business Associate requirements of the Privacy Rule and the Security Rule and the **HITECH** BA Provisions, including, but not limited to, the Business Associate contract requirements at 45 C.F.R. §164.308(b), §164.314(a), §164.502(e), §164.504(e), and as may be amended; and

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

- 1. Definitions.** Unless otherwise provided in this BAA, capitalized terms have the same meanings as set forth in **HIPAA**, the Privacy Rule, the Security Rule, the Breach Notification Rule, the Omnibus Rule or the **HITECH** BA Provisions (collectively, the “**HIPAA** Requirements”).

2. **Scope of Use and Disclosure by VENDOR of PHI.** VENDOR shall be permitted to Use and Disclose PHI that is disclosed to it by CLIENT as necessary to perform the services in accordance with the HIPAA Requirements.
3. **Obligations of VENDOR.** In connection with VENDOR'S Use and Disclosure of PHI, VENDOR agrees that it will comply with the following and it will ensure that each individual provided to CLIENT under the terms of the Agreement will:
 - a. Use or further Disclose PHI only as permitted or required by this BAA or as Required by Law;
 - b. Comply with all applicable CLIENT policies and procedures related to the privacy and security of PHI;
 - c. Use reasonable and appropriate safeguards and comply, where applicable, with the Security Rule with respect to electronic PHI, to prevent Use or Disclosure of PHI other than as provided for by this BAA, including implementation of the Administrative, Physical and Technical Safeguards and the Organizational Requirements of the Security Rule (45 C.F.R. §§164.306-316) that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic PHI that it creates, receives, maintains or transmits on behalf of CLIENT or any Covered Entity;
 - d. Mitigate any harmful effect that is known to VENDOR of a Use or Disclosure of PHI by VENDOR in violation of this BAA;
 - e. Promptly report to CLIENT as soon as practicable, but in any event no later than five (5) business days after becoming aware of, any Use or Disclosure of PHI not provided for in or in violation of this BAA, any Security Incident as that term is defined in the Security Rule, and any Breach of Unsecured PHI as that term is defined in the Breach Notification Rule of which VENDOR becomes aware;
 - f. Require that any VENDOR subcontractor that creates, receives, maintains or transmits PHI on behalf of CLIENT or a Covered Entity agrees to the same restrictions and conditions that apply to VENDOR with respect to such PHI in accordance with the applicable HIPAA Requirements;
 - g. Within five (5) days of receiving a written request from a Covered Entity or CLIENT, make available the PHI in a Designated Record Set to CLIENT or the Covered Entity or, if so directed by either of them, to an Individual in order to meet the access requirements under 45 C.F.R. 164.524;
 - h. Within five (5) days of receiving a written request from CLIENT or a Covered Entity, make PHI available for amendment and incorporate any amendment to the PHI in accordance with the Privacy Rule in the event that the PHI in VENDOR'S possession constitutes a Designated Record Set;
 - i. Make internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received by VENDOR on behalf of, CLIENT or any Covered Entity available to the Secretary of HHS, in a reasonable time and manner as designated by the Secretary of HHS, CLIENT or Covered Entity, for purposes of the Secretary of HHS determining Business Associate or Covered Entity's compliance with the HIPAA Requirements. In addition, upon written request by CLIENT, make its internal practices, books and records relating to compliance with the HIPAA Requirements available to CLIENT for purposes of determining CLIENT'S compliance with the HIPAA Requirements;
 - j. Document such disclosures of PHI and information related to such disclosures, in order for CLIENT or Covered Entity to respond to a request by an Individual or by CLIENT on behalf of an Individual or Covered Entity for an accounting of disclosures, in accordance with 45 C.F.R. 164.528;
 - k. Within five (5) days of receiving a request from CLIENT or a Covered Entity, make available the information necessary for the Covered Entity to make an accounting of Disclosures of PHI about an individual;

- l. To the extent that CLIENT is to carry out an obligation of the Covered Entity under the Privacy Rule and the services to be provided by VENDOR hereunder are part of such an obligation, VENDOR shall comply with the requirements of the Privacy Rule that apply to CLIENT and Covered Entity in the performance of such obligation; and
- m. VENDOR hereby acknowledges its status as a Business Associate as described in the Omnibus Rule. VENDOR hereby acknowledges and agrees that VENDOR shall be subject to each of the HITECH BA Provisions with respect to VENDOR'S role as a Business Associate. CLIENT and the VENDOR each further agree that the provisions of HITECH that apply to Business Associates that are required to be incorporated by reference in a business associate agreement are hereby incorporated into this BAA.

4. Termination.

- a. Termination for Breach. In the event CLIENT determines that VENDOR may have breached a material term of this BAA, CLIENT may terminate this BAA and any related agreements between the Parties.
 - b. Automatic Termination. This BAA will automatically terminate without any further action by the Parties upon the termination or expiration of any related agreement between the Parties.
 - c. Effect of Termination. Upon termination of this BAA, VENDOR will return or destroy all PHI received from CLIENT or created or received by VENDOR on behalf of CLIENT. VENDOR shall not maintain or retain any copies of such PHI.
 - d. Survival. The obligations of VENDOR under Section 4.c and Section 6 of this BAA shall survive any termination or expiration of this BAA.
- 5. Effect of Agreement.** With respect solely to the subject matter herein, in the case of any conflict in terms between this BAA and any other agreement between the Parties, the terms of this BAA shall control and supersede and nullify any conflicting terms as it relates to the Parties in a Business Associate relationship.
- 6. Indemnification.** VENDOR shall defend, indemnify and hold harmless CLIENT, its affiliates, officers, directors, employees and agents, from and against any claims or liabilities, and shall pay all losses, damages, liabilities, claims and actions, and all related expenses (including reasonable attorneys' fees and expenses) based on or arising out of any breach or alleged breach by VENDOR or any employee, agent or subcontractor of VENDOR of any duty or obligation of the BAA that pertains in any way, directly or indirectly, to PHI or the protection of the confidentiality thereof. VENDOR will reimburse CLIENT for all costs, expenses and damages (including reasonable attorneys' fees) associated with any notification process that may be required under the HIPAA Requirements or other applicable state or federal law with respect to any Breach of Unsecured PHI or any breach of any other federal or state law by VENDOR or any of its employees, agents or subcontractors.
- 7. Training.** VENDOR agrees that VENDOR will fully train its employees, subcontractors, or agents who will provide the services under the Agreement on the HIPAA Privacy and Security Rules. In the event that VENDOR is unable to provide this required training, VENDOR will notify CLIENT and require its employees, subcontractors, or agents to take the CLIENT'S HIPAA training. VENDOR agrees that its employees, subcontractors, or agents will attend any additional training as deemed necessary by CLIENT.
- 8. Reporting.** Notwithstanding anything contained in the Agreement or this BAA to the contrary, the provisions provided herein are not intended to restrict or prevent CLIENT from fulfilling its

obligation, if any, to make certain disclosures to public officials or authorities having jurisdiction (including but not limited to OCR or CMS).

9. **No Third Party Beneficiaries.** Nothing express or implied in this BAA 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.
10. **Independent Contractor.** Unless and to the extent otherwise expressly agreed in writing by both Parties to this BAA, VENDOR is an independent contractor and not an agent of CLIENT or any Covered Entity.
11. **Entire Agreement.** This BAA constitutes the entire understanding and obligation of the Parties with respect to the subject matter hereof and supersedes any prior agreements, writings or understandings, whether oral or written with respect to the subject matter hereof.
12. **Effective Date.** This BAA shall be effective as of the effective date of the Agreement.