

# HIPAA SUBCONTRACTOR AGREEMENT

This HIPAA Subcontractor Agreement, dated as of \_\_\_\_\_, 20\_\_\_\_ (“Agreement”) supplements and is made a part of an underlying agreement between the Business Associate and a Covered Entity.

This Agreement is by and between \_\_\_\_\_, (“**Business Associate**”) and \_\_\_\_\_, (“**Subcontractor**”). Business Associate and Subcontractor may be referred to herein collectively as the “Parties” or individually as “Party”.

**WHEREAS**, Business Associate and Subcontractor are Parties to an agreement or various agreements pursuant to which Subcontractor provides certain services to Business Associate. In connection with such services, Subcontractor creates, receives, maintains or transmits Protected Health Information from or on behalf of Business Associate or a Covered Entity, which information is subject to protection under the Federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104 191 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”), and related regulations promulgated by the Secretary (“HIPAA Regulations”); and

**WHEREAS**, Business Associate qualifies as a “business associate” (as defined by the HIPAA Regulations) of its clients, which means that Business Associate has certain responsibilities with respect to the Protected Health Information of its clients; and

**WHEREAS**, in light of the foregoing and the requirements of HIPAA, the HITECH Act, and HIPAA Regulations, Subcontractor and Business Associate agree to be bound by the following terms and conditions.

**NOW, THEREFORE**, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Definitions.

a. General. Terms used, but not otherwise defined, in this Agreement shall have the same meaning given to those terms by HIPAA, the HITECH Act, and HIPAA Regulations as in effect or as amended from time to time.

b. Specific.

i. Breach. “Breach” shall have the same meaning as the term “breach” in 45 CFR § 164.402.

ii. Covered Entity. “Covered Entity” shall have the same meaning as the term “covered entity” in 45 CFR § 160.103, limited to the Covered Entities that are clients of Business Associate.



iii. Electronic Health Record. “Electronic Health Record” shall have the same meaning as the term “electronic health record” in the HITECH Act, Section 13400(5).

iv. Electronic Protected Health Information. “Electronic Protected Health Information” shall have the same meaning as the term “electronic protected health information” in 45 CFR § 160.103, limited to the information that Subcontractor creates, receives, maintains, or transmits from or on behalf of Business Associate or a Covered Entity.

v. Individual. “Individual” shall have the same meaning as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

vi. Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164.

vii. Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103, limited to the information created, received, maintained or transmitted by Subcontractor from or on behalf of Business Associate or a Covered Entity.

viii. Qualified Service Organization Agreement. “Qualified Service Organization Agreement” shall have the same meaning as defined in 42 CFR 2.12(c)(4).

x. Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

xi. Security Rule. “Security Rule” shall mean the Security Standards at 45 CFR Part 160 and Part 164.

xii. Services Agreement. For purposes of this Agreement, “Services Agreement” shall refer to any present or future agreements between Business Associate and Subcontractor, either written or oral, under which Subcontractor provides services to Business Associate or its clients which involve the use or disclosure of Protected Health Information. The Services Agreement is amended by and incorporates the terms of this Agreement.

xiii. Subcontractor Vendor. “Subcontractor Vendor” shall have the same meaning as the term “subcontractor” in 45 CFR § 160.103.

xiv. Unsecured Protected Health Information. “Unsecured Protected Health Information” shall have the same meaning as the term “unsecured protected health information” in 45 CFR § 164.402.

## 2. Obligations and Activities of Subcontractor.

a. Use and Disclosure. Subcontractor agrees not to use or disclose Protected Health Information other than as permitted or required by the Services Agreement, this Agreement or as required by law. Notwithstanding the foregoing sentence, Subcontractor agrees to adhere to the terms and conditions of any Business Associate Agreements between Business Associate and any Covered Entity which apply to Protected Health Information. Subcontractor represents and warrants that he/she/it is familiar with the requirements of HIPAA, the HITECH Act and HIPAA Regulations regarding Business Associates and Business Associate Agreements. Subcontractor shall comply with the provisions of this Agreement relating to privacy and security of Protected Health Information and all present and future provisions of HIPAA, the HITECH Act and HIPAA Regulations that relate to the privacy and security of Protected Health Information and that are applicable to Covered Entity and/or Business Associate. Without limiting the foregoing, to the extent the Subcontractor will carry out one or more of the Covered Entity's or Business Associate's obligations under the Privacy Rule, Subcontractor shall comply with the requirements of the Privacy Rule that apply to the Covered Entity and/or Business Associate in the performance of such obligations.

b. Qualified Service Organization. Subcontractor acknowledges that it may also be a Qualified Service Organization as defined in 42 CFR 2.11 and as such: (i) acknowledges that, to the extent it receives, stores, processes or otherwise deals with any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug program, it is fully bound by the regulations in 42 CFR Part 2; and (ii) if necessary, will resist in judicial proceedings any efforts to obtain access to any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug program, except as permitted by 42 CFR Part 2.

c. Appropriate Safeguards. Subcontractor agrees to use appropriate safeguards and comply, where applicable, with the Security Rule to prevent the use or disclosure of the Protected Health Information other than as permitted by this Agreement. Without limiting the generality of the foregoing, Subcontractor will:

i. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information as required by the Security Rule; and

ii. Ensure that any Subcontractor Vendor to whom Subcontractor provides Electronic Protected Health Information agrees in writing to implement reasonable and appropriate safeguards and comply, where applicable, with the Security Rule to protect Electronic Protected Health Information and comply with the other requirements of Section 2(a) above.

d. Reporting. Subcontractor agrees to promptly, and in any event within three (3) business days, report to Business Associate any of the following:

i. Any use or disclosure of Protected Health Information not permitted by this Agreement of which Subcontractor becomes aware.

- ii. Any Security Incident of which Subcontractor becomes aware.
- iii. The discovery of a Breach of Unsecured Protected Health Information.

A Breach is considered “discovered” as of the first day on which the Breach is known, or reasonably should have been known, to Subcontractor or any employee, officer or agent of Subcontractor, other than the individual committing the Breach. Any notice of a Security Incident or Breach of Unsecured Protected Health Information shall include the identification of each Individual whose Protected Health Information has been, or is reasonably believed by Subcontractor to have been, accessed, acquired, or disclosed during such Security Incident or Breach as well as any other relevant information regarding the Security Incident or Breach. Any such notice shall be directed to Business Associate pursuant to the notice provisions of the Services Agreement or to the Privacy Officer of Business Associate.

e. Mitigation. Subcontractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Subcontractor of a use or disclosure of Protected Health Information by Subcontractor or its employees, officers, Subcontractor Vendors or agents in violation of the requirements of this Agreement (including, without limitation, any Security Incident or Breach of Unsecured Protected Health Information). Subcontractor shall keep Business Associate fully apprised of all mitigation efforts of the Subcontractor required under this Section 2(e).

f. Subcontractor Vendor. Subcontractor shall ensure that any Subcontractor Vendor to whom Subcontractor provides Protected Health Information received from, or created, maintained, received or transmitted by, Subcontractor on behalf of Business Associate or a Covered Entity agrees in writing to the same terms and conditions that apply to Protected Health Information pursuant to this Agreement.

g. Access to Designated Record Sets. To the extent that Subcontractor possesses or maintains Protected Health Information in a Designated Record Set, Subcontractor agrees to provide access to such Protected Health Information at the request of Business Associate, within three (3) business days of such request, to Business Associate or, as directed by Business Associate, to a Covered Entity or an Individual in order to meet the requirements under HIPAA Regulations. If an Individual makes a request for access to Protected Health Information directly to Subcontractor, Subcontractor shall notify Business Associate of the request within three (3) business days of such request and will cooperate with Business Associate and any Covered Entity and allow Business Associate or such Covered Entity to send the response to the Individual.

h. Amendments to Designated Record Sets. To the extent that Subcontractor possesses or maintains Protected Health Information in a Designated Record Set, Subcontractor agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Business Associate or a Covered Entity directs or agrees to in accordance with HIPAA, HIPAA Regulations or the HITECH Act, within three (3) business days of any such request. If an Individual makes a request for an amendment to Protected Health Information directly to Subcontractor, Subcontractor shall notify Business Associate of

the request within three (3) business days of such request and will cooperate with Business Associate and any Covered Entity and allow Business Associate or the Covered Entity to send the response to the Individual.

i. Access to Books and Records. Subcontractor agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Subcontractor on behalf of Business Associate or a Covered Entity available to Business Associate, or at the request of Business Associate, to a Covered Entity or to the Secretary, within three (3) business days of such request or in the time and manner otherwise designated by the Secretary, for purposes of the Secretary determining the Business Associate or Covered Entity's compliance with the Privacy Rule.

j. Accountings. Subcontractor agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entities to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with HIPAA, HIPAA Regulations and the HITECH Act.

k. Requests for Accountings. Subcontractor agrees to provide to Business Associate, or at the direction of Business Associate, to a Covered Entity or an Individual, within fifteen (15) days of a request by Business Associate, information collected in accordance with Section 2(j) of this Agreement, to permit a Covered Entity or Business Associate to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with HIPAA, HIPAA Regulations and the HITECH Act. If an Individual makes a request for an accounting directly to Subcontractor, Subcontractor shall notify Business Associate of the request within three (3) business days of such request and will cooperate with Business Associate and any Covered Entity and allow Business Associate or the Covered Entity to send the response to the Individual.

### 3. Permitted Uses and Disclosures by Subcontractor.

a. Services Agreement. Except as otherwise limited in this Agreement, Subcontractor may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, a Covered Entity or the Business Associate as specified in the Services Agreement, provided that such use or disclosure would not violate HIPAA, the HITECH Act or HIPAA Regulations if done by Business Associate or a Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

b. Use for Administration of Subcontractor. Except as otherwise limited in this Agreement, Subcontractor may use Protected Health Information for the proper management and administration of the Subcontractor or to carry out the legal responsibilities of the Subcontractor.

c. Disclosure for Administration of Subcontractor. Except as otherwise limited in this Agreement, Subcontractor may disclose Protected Health Information for the proper

management and administration of the Subcontractor, provided that (i) disclosures are required by law, or (ii) Subcontractor obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Subcontractor and Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Permissible Requests by Covered Entity. Except as set forth in Section 3 of this Agreement, Business Associate shall not request Subcontractor to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by the Business Associate or any of its client Covered Entities.

5. Term and Termination.

a. Term. This Agreement shall be effective as of the date of this Agreement and shall terminate when all of the Protected Health Information provided by Business Associate or a Covered Entity to Subcontractor, or created, received or maintained by Subcontractor on behalf of Business Associate or a Covered Entity, is destroyed or returned to Business Associate or a Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

b. Termination for Cause. Upon Business Associate's knowledge of a material breach by Subcontractor of this Agreement, Business Associate shall either:

i. Provide an opportunity for Subcontractor to cure the breach or end the violation and terminate this Agreement and the Services Agreement if Subcontractor does not cure the breach or end the violation within the time specified by Business Associate; or

ii. Notwithstanding anything contained in the Services Agreement to the contrary, immediately terminate this Agreement and the Services Agreement if Subcontractor has breached a material term of this Agreement and cure is not possible.

c. Effect of Termination.

i. Except as provided in Section 5(c)(ii), upon termination of the Services Agreement or this Agreement for any reason, Subcontractor shall return to Business Associate or destroy all Protected Health Information received from Business Associate or a Covered Entity, or created or received by Subcontractor on behalf of Business Associate or a Covered Entity. This provision shall apply to Protected Health Information that is in the possession of Subcontractor Vendors or agents of Subcontractor. Subcontractor shall retain no copies of the Protected Health Information.

ii. In the event that Subcontractor determines that returning or destroying the Protected Health Information is infeasible, Subcontractor 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 Protected Health Information is infeasible, Subcontractor shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Subcontractor maintains such Protected Health Information.

6. Indemnity. Subcontractor agrees to indemnify, defend and hold harmless Business Associate and its client Covered Entities and each of their respective employees, directors/trustees, members, professional staff, representatives and agents (collectively, the "Indemnitees") from and against any and all claims (whether in law or in equity), obligations, actions, causes of action, suits, debts, judgments, losses, fines, penalties, damages, expenses (including attorney's fees), liabilities, lawsuits or costs incurred by the Indemnitees which arise or result from a breach of the terms and conditions of this Agreement or a violation of HIPAA, the HITECH Act or HIPAA Regulations by Subcontractor or its employees or agents.

7. Electronic Transaction Standards. To the extent that Subcontractor or its products perform all or part of any transaction for which the Secretary has adopted a standard under HIPAA ("Covered Transactions") on the Business Associate's behalf, the following shall apply:

a. Compliance with HIPAA Standards. When providing its services and/or products, Subcontractor shall comply with all applicable HIPAA standards and requirements (including, without limitation, those specified in 45 CFR Part 162) with respect to the transmission of health information in electronic form in connection with any transaction for which the Secretary has adopted a standard under HIPAA ("Covered Transactions"). Subcontractor will make its services and/or products compliant with HIPAA's standards and requirements no less than thirty (30) days prior to the applicable compliance dates under HIPAA. Subcontractor represents and warrants that it is aware of all current HIPAA standards and requirements regarding Covered Transactions, and Subcontractor shall comply with any modifications to HIPAA standards and requirements which become effective from time to time. Subcontractor agrees that such compliance shall be at its sole cost and expense, which expense shall not be passed on to Business Associate in any form, including, but not limited to, increased fees.

b. Agents and Subcontractors. Subcontractor shall require all of its agents and subcontractors (if any) who assist Subcontractor in providing its services and/or products to comply with the terms of this Section 7.

8. Coordination of Subcontractor and Business Associate.

a. Investigation. Subcontractor shall reasonably cooperate and coordinate with Business Associate and any Covered Entity in the investigation of any violation of the requirements of this Agreement and/or any Security Incident or Breach.

b. Reports and Notices. Subcontractor shall reasonably cooperate and coordinate with Business Associate and any Covered Entity in the preparation of any reports or notices

to the Individual, a regulatory body or any third party required to be made under HIPAA, HIPAA Regulations, the HITECH Act, or any other Federal or State laws, rules or regulations, provided that any such reports or notices shall be subject to the prior written approval of Covered Entity.

9. Miscellaneous.

a. No HIPAA Agency Relationship. It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Business Associate and Subcontractor for purposes of liability under HIPAA, HIPAA Regulations, or the HITECH Act. No terms or conditions contained in this Agreement shall be construed to make or render Subcontractor an agent of Business Associate.

b. Regulatory References. A reference in this Agreement to a section in HIPAA, the HITECH Act, or the HIPAA Regulations means the section as in effect or as amended or modified from time to time, including any corresponding provisions of subsequent superseding laws or regulations.

c. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Business Associate and its Covered Entity clients to comply with the requirements of HIPAA, the HITECH Act, and HIPAA Regulations.

d. Survival. The rights and obligations of Subcontractor under Sections 5(c), 6, 8 and 9 of this Agreement shall survive the termination of the Services Agreement and this Agreement.

e. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Business Associate and its client Covered Entities to comply with HIPAA, HIPAA Regulations and the HITECH Act.

f. Miscellaneous. The terms of this Agreement are hereby incorporated into the Services Agreement (including present and future agreements). Except as otherwise set forth in Section 9(e) of this Agreement, in the event of a conflict between the terms of this Agreement and the terms of the Services Agreement, the terms of this Agreement shall prevail. Subcontractor's obligations hereunder shall not be subject to any limitations of liability or remedies in the Services Agreement. The terms of the Services Agreement which are not modified by this Agreement shall remain in full force and effect in accordance with the terms thereof. This Agreement shall be governed by, and construed in accordance with, the laws of the state where the Business Associate is located, exclusive of conflict of law rules. Each Party hereby agrees and consents that any legal action or proceeding with respect to this Agreement shall only be brought in the courts of the state where the Business Associate is located in the county where the Business Associate is located. The Services Agreement together with this Agreement constitutes the entire agreement between the Parties with respect to the subject matter contained herein, and this Agreement supersedes and replaces



any former service agreement or addendum entered into by the Parties. This Agreement may be executed in counterparts, each of which when taken together shall constitute one original. Any PDF or facsimile signatures to this Agreement shall be deemed original signatures to this Agreement. No amendments or modifications to the Agreement shall be effective unless agreed upon by both parties in writing.

**IN WITNESS WHEREOF**, the Parties have caused this Business Associate Subcontractor Agreement to be executed in by their duly authorized representatives.

**Business Associate:** \_\_\_\_\_ **Date:** \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

**Subcontractor:** \_\_\_\_\_ **Date:** \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_