**BUSINESS ASSOCIATE**

**PRIVACY AND SECURITY ADDENDUM**

 This Business Associate Addendum (“**Addendum**”), effective \_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_ (“**Effective Date**”), is entered into by and between University of Southern California, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**University**”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**Vendor**”). Capitalized terms used in this Addendum without definition shall have the respective meanings assigned to such terms by the Administrative Simplification section of the Health Insurance Portability and Accountability Act and their implementing regulations as each may be amended from time to time (collectively, “**HIPAA**”).

**RECITALS**

 A. University is a “**Covered Entity**” and Vendor is a “**Business Associate**” within the meaning of HIPAA.

 B. The parties hereto desire to enter into this Addendum to memorialize their obligations with respect to Protected Health Information that Vendor transmits, receives, maintains, creates, uses or discloses on behalf of University (“**PHI**”), including, without limitation, PHI transmitted or maintained in Electronic Media (“**ePHI**”).

 In consideration of the mutual promises and agreements below and in order to comply with all legal requirements for the protection of this information, the parties hereto agree as follows:

**I. DEFINITIONS**

 The following terms used in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (also referred to herein as “PHI”), Electronic Protected Health Information (also referred to herein as ePHI”), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information (also referred to herein as “Unsecured PHI”), Limited Data Set, Research, Health Care Operations, Confidentiality, Integrity, Availability, Standard Transaction, Confidentiality, Availability, Integrity and Use. Business Associate shall have the meaning given to such term pursuant to 45 C.F.R. § 160.103, and in reference to the party to this BAA shall mean the first Party listed above. Covered Entity shall have the meaning given to such term pursuant to 45 C.F.R. § 160.103, and in reference to the party to this BAA shall mean the second Party listed above.

**II. GENERAL PROVISIONS**

Section 1. **Effect**. This Addendum supplements, modifies and amends any and all agreements (the “**Agreement(s)**”), whether oral or written, between the parties involving the receipt, transmission, maintenance, use or disclosure of PHI by Vendor on behalf of University. The terms and provisions of this Addendum shall supersede any other conflicting or inconsistent terms and provisions in any Agreement(s) between the parties, including all exhibits or other attachments thereto and all documents incorporated therein by reference.

 Section 2. **Amendment**. The parties acknowledge and agree that the Health Information Technology for Economic and Clinical Health Act and its implementing regulations impose requirements with respect to privacy, security and breach notification applicable to Business Associates (collectively, the “**HITECH BA Provisions”**). The HITECH BA Provisions and any other future amendments to HIPAA affecting Business Associate Agreements are hereby incorporated by reference into this Addendum as if set forth in this Addendum in their entirety, effective on the later of the effective date of this Addendum or such subsequent date as may be specified by HIPAA.

**III. OBLIGATIONS OF VENDOR**

 Section 1. **Use and Disclosure of Protected Health Information**.Vendor may use, access, and disclose PHI only as required to satisfy its obligations under the Agreement, as permitted herein, or required by law, but shall not otherwise use or disclose any PHI. Vendor shall not use, access, or disclose PHI received from University in any manner that would constitute a violation of the HIPAA if used by University, except that Vendor may use PHI

1. for Vendor’s proper management and administrative services,
2. to carry out the legal responsibilities of Vendor or
3. to provide data aggregation services relating to the health care operations of University if required under the Agreement,
4. to de-identify any and all PHI created or received from University under the Agreement(s) ; provided, however, that the de-identification conforms to the requirements of 45 CFR 164.514(b). Vendor is required to demonstrate that PHI has been de-identified in accordance with requirements of 45 CFR 164.514(b), upon request from University. De-identified data remains the sole property of the University and will not be further disclosed.

Vendor acknowledges that all PHI shall be and remain the sole property of University, including any and all forms thereof developed by Vendor in the course of its fulfillment of its obligations pursuant to this Agreement. Vendor further represents that, to the extent Vendor requests that University disclose PHI to Vendor, such a request is only for the minimum necessary PHI for the accomplishment of Vendor’s purpose. To the extent Vendor carries out any of University’s obligations under HIPAA, Vendor shall comply with the requirements of HIPAA that apply to University in the performance of such obligations.

Vendor or its agents or Subcontractors shall not perform any work or provide any services outside the United States of America that involves access to, use of, storage of or disclosure of, PHI without the prior written consent of University in each instance.

 Section 2. **Safeguards Against Misuse of Information**. Vendor agrees that it will use all appropriate safeguards to prevent the use or disclosure of PHI other than pursuant to the terms and conditions of this Addendum. Vendor further agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that the Vendor creates, receives, maintains, or transmits on behalf of University. Vendor shall comply with the HIPAA Security Rule with respect to ePHI.

 Section 3. **Reporting**.Vendor shall, as soon as practicable, but in no event later than within 24 hours of becoming aware of any use or disclosure of PHI in violation of the Addendum, report any such disclosure to University. In such event, the Vendor shall, in consultation with University, mitigate, to the extent practicable, any harmful effect that is known to the Vendor of such improper use or disclosure.

In addition, Vendor must report to University any Security Incident or Breach of which it becomes aware in the following time and manner: (a) any Security Incident will be reported to University Office of Compliance (3500 S. Figueroa St., UGB 105 Los Angeles, CA 90089-8007 Tel. (213) 740-8258 Fax (213) 740-9657) in writing, within one (1) business day of the date on which Vendor first becomes aware of such Security incident, and (b) any Breach of PHI (whether electronic, oral or in any other medium and whether secure or unsecured) shall be reported to University Office of Compliance within one (1) business day of the date on which Vendor first becomes aware of such Breach.

Vendor will cooperate fully with the University in investigating any potential or actual breaches, including assistance, if requested, in conducting any harm threshold risk analyses.

Vendor will reimburse University for all costs, expenses and damages (including reasonable attorney’s fees) associated with any notification process that may be required under the HITECH BA Provisions with respect to any Breach of Unsecured PHI caused by Vendor or its subcontractors.

 Section 4. **Designation of Security Contact**. Vendor agrees to designate an appropriate employee of the Vendor (the “**Vendor Security Contact**”) reasonably acceptable to University to address all security issues with respect to University that may arise under the Agreement.

 Section 5. **Agreements by Third Parties**. Vendor shall obtain and maintain a written agreement meeting the requirements of 45 C.F.R. §§ 164.504 (e) and 164.314(a)(2) with each Subcontractor (including, without limitation, a Subcontractor that is an agent under applicable law) that creates, receives, maintains or transmits PHI on behalf of Vendor. Vendor shall ensure that the written agreement with each Subcontractor obligates the Subcontractor to comply with same restrictions, terms and conditions that apply to Vendor pursuant to this Agreement with respect to such PHI.

 Section 6. **Access to Information**. Within five (5) business days of a request by University for access to PHI about an individual contained in a Designated Record Set, Vendor shall make available to University such PHI for so long as such information is maintained in the Designated Record Set. In the event any individual requests access to PHI directly from Vendor, Vendor shall within two (2) business days forward such request to University. Any denials of access to the PHI requested shall be the responsibility of University.

 Section 7. **Availability of Protected Health Information for Amendment**. Within ten (10) days of receipt of a request from University for the amendment of an individual’s PHI or a record regarding an individual contained in a Designated Record Set (for so long as the PHI is maintained in the Designated Record Set), Vendor shall provide such information to University for amendment and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

 Section 8. **Accounting of Disclosures**. Within ten (10) days of notice by University to Vendor that it has received a request for an accounting of disclosures of PHI, other than related to the treatment of the patient, the processing of payments related to such treatment, or the operation of a covered entity or its business associate and not relating to disclosures made earlier than six (6) years prior to the date on which the accounting was requested, Vendor shall make available to University such information as is in Vendor’s possession and is required for University to make the accounting required by 45 C.F.R. §164.528. At a minimum, Vendor shall provide University with the following information: (i) the date of the disclosure, (ii) the name of the entity or person who received the 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 such disclosure which includes an explanation of the basis for such disclosure. In the event the request for an accounting is delivered directly to Vendor, Vendor shall within two (2) days forward such request to University. Vendor hereby agrees to implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section. To the extent Vendor maintains or operates an electronic health record system on behalf of University and as of the Applicable Effective Date, Vendor shall also maintain information for the preceding three (3) year period (but no earlier than the Applicable Effective Date) sufficient to enable University to make an accounting of disclosures for treatment, payment and health care operations.

 Section 9. **Restrictions; Limitations in Notice of Privacy Practices**. Vendor shall comply with any reasonable limitation in University’s Notice of Privacy Practices to the extent that such limitation affects Business Associate’s receipt, transmission, maintenance, use or disclosure of PHI under an Agreement. Vendor shall comply with any reasonable restriction on the use or disclosure of PHI that University has agreed to or is required to abide by under 45 CFR § 164.522, to the extent that such restriction affects Vendor’s receipt, transmission, maintenance, use or disclosure of PHI. University shall promptly notify Vendor of any limitation(s) in its Notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Vendor’s use, access, or disclosure of PHI.

 Section 10. **Availability of Books and Records**. Vendor hereby agrees to make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Vendor on behalf of, University available to the Secretary, promptly upon request, and no later than ten (10) calendar days, for purposes of determining and facilitating University’s and Vendor’s compliance with HIPAA. In addition, upon request by University, Vendor shall make its internal practices, books and records relating to compliance with the HITECH BA Provisions available to University for purposes of determining the Vendor’s compliance with the HITECH BA Provisions. Without limiting the generality of the foregoing, Vendor acknowledges and agrees that as of the Applicable Effective Date, Vendor shall have policies and procedures that are sufficient to comply with the applicable requirements of the HITECH BA Provisions.

 Section 11. **Third Party Audit Rights**. Vendor shall have an independent review, by internal or external auditors, of administrative, physical and technical safeguards and technological mechanisms comprising its security risk management program no less than annually, in accordance with current industry standards and shall cure such deficiencies in a timely manner. Vendor shall provide University with a copy of such reports, at University’s request.

 Section 12. **Compliance with Red Flag Rules**. Vendor and University acknowledge that University may be subject to certain identity theft detection regulations promulgated by the Federal Trade Commission, commonly known as the Red Flag Rules. As a contractor to University, Vendor agrees that, to the extent any red flags for detecting identity theft exist, Vendor shall implement an identity theft program sufficient to detect such red flags and prevent and mitigate identity theft. University reserves the right to request a copy of Vendor’s identity theft prevention program policies (“**ID Theft Policies**”) and Vendor will provide a copy of the ID Theft Policies within fifteen (15) days of receiving such request.

 Section 13. **PCI Compliance**. Vendor agrees that during the term of the Agreement and to the extent applicable, Vendor shall comply with all applicable requirements to be considered Payment Card Industry Data Security Standard (“PCI DSS”) compliant, and has performed the necessary steps to validate its compliance with the PCI DSS. Upon the request of University, Vendor shall provide University with evidence of Vendor’s compliance with PCI DSS, such as an Attestation of Compliance or applicable completed self-assessment questionnaire (SAQ).

Section 14. **Notice of Request for Data**. Vendor agrees to notify University within five (5) business days of Vendor’s receipt of any request or subpoena for PHI. To the extent that University decides to assume responsibility for challenging the validity of such request, Vendor agrees to cooperate fully with University in such challenge.

 Section 15. **Injunction**. Vendor hereby agrees that University will suffer irreparable damage upon Vendor’s breach of this Addendum and that such damages shall be difficult to quantify. Vendor hereby agrees that University may seek an injunction to enforce the terms of this Addendum against Vendor, in addition to any other remedy University may have.

**IV. TERM AND TERMINATION**

Section 1. **Term**. This Addendum shall become effective on the Effective Date and, unless otherwise terminated as provided herein, shall have a term that shall run concurrently with that of the last expiration date or termination of the Agreement(s).

 Section 2. **Termination Upon Breach of Provisions Applicable to Protected Health Information**. Any other provision of the Agreement(s) notwithstanding, this Addendum and the Agreement(s) may be terminated by University upon thirty (30) days written notice to Vendor in the event that Vendor breaches any material provision contained in this Addendum and such breach is not cured within such thirty (30) day period; provided, however, that in the event that termination of the Agreement (s) is not feasible, in University’s sole discretion, Vendor acknowledges and agrees that University has the right to report the breach to the Secretary, notwithstanding any other provision of the Agreement(s) to the contrary.

 If and to the extent requested by University, Vendor shall continue to perform the services required by the Agreement on a limited basis and/or assist University in transitioning such services and any related PHI or other data to University or to a third party designated by University for a reasonable charge (not to exceed the amount charged for performing such services pursuant to the Agreement).

The Vendor agrees to defend, indemnify, and hold harmless University against any and all claims, liabilities, judgments or damages asserted against, imposed upon or incurred by University that arise out of any violation by the Vendor of its obligations under this Agreement.

Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever, except for indemnity rights and remedies for the University.

 Section 3. **Effect of Termination**. Upon termination of this Addendum, Vendor shall either return or destroy all PHI received from University or created or received by Vendor on behalf of University and which Vendor still maintains in any form. Vendor shall not retain any copies of such PHI. Notwithstanding the foregoing, to the extent that University agrees that it is not feasible to return or destroy such PHI, the terms and provisions of this Addendum shall survive termination of the Agreement(s) and such PHI shall be used, accessed, or disclosed solely for such purpose or purposes which prevented the return or destruction of such PHI.

 **INTENDING TO BE LEGALLY BOUND,** the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

**VENDOR UNIVERSITY**

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

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