UNIVERSITY OF CALIFORNIA

APPENDIX – HIPAA BUSINESS ASSOCIATE

ARTICLE 1 – GENERAL

A. UC and Supplier desire to protect the privacy and provide for the security of Protected Health Information (as that term is defined herein) used by or disclosed to Supplier in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the regulations promulgated thereunder by the U.S. Department of Health and Human Services (45 CFR Parts 160, 162 and 164, the HIPAA Regulations), the Health Information Technology for Economic and Clinical Health Act of 2009 (the HITECH Act), California Health and Safety Code §1280.15, California Civil Code §§1798.82 and 1798.29, and other applicable laws and regulations. The purpose of this Appendix is to satisfy certain standards and requirements of HIPAA, the HIPAA Regulations, including 45 CFR § 164.504(e), and the HITECH Act, including Subtitle D, part 1, as they may be amended from time to time.

B. Supplier is or may be a Business Associate as defined under HIPAA. UC wishes to disclose to Supplier certain information, some of which may constitute Protected Health Information or Medical Information. UC has designated all of its HIPAA health care components as a single component of its hybrid entity and therefore this Appendix is binding on all other UC health care components (collectively, the Single Health Care Component or the SHCC). This Appendix is effective on the date of the Agreement under which Supplier provides Goods and/or Services to UC (Effective Date).

C. This Appendix applies only if and to the extent Supplier is functioning as a Business Associate to the SHCC.

ARTICLE 2 – DEFINITIONS

Except as set forth in this Article 2, capitalized terms used in this Appendix shall have the meaning provided by HIPAA, the HIPAA Regulations, the HITECH Act, California Health and Safety Code §§ 1798.82 and 1798.29, and other applicable laws and regulations.

A. "Agent" means a person or entity, including a sub-supplier or Workforce Member, who has an agency relationship to Supplier and who is required to receive Protected Health Information or Medical Information to provide the Goods and/or Services in the Agreement.

B. "Breach" means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information, and shall have the meaning given to such term under HIPAA and the HIPAA regulations, including 45 CFR §164.402, as well as California Civil Code §§ 1798.29 and 1798.82.

C. "Destruction" means the use of a technology or methodology by which the media on which the PHI is stored or recorded has been shredded, destroyed, cleared, or purged, as appropriate, such that the PHI cannot be read, retrieved, or otherwise reconstructed. Redaction is inadequate for the purposes of destruction.

D. "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given to such term under the HITECH Act, including Section 13400(5).

E. “Electronic PHI” means PHI that is transmitted by or maintained in electronic media and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 160.103. For the purposes of this Appendix, Electronic PHI includes all computerized data, as defined in California Civil Code §§ 1798.29 and 1798.82.

F. “Encryption” means a technology or methodology that utilizes an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key, and such confidential process or key that might enable decryption has not been breached, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.304.

G. "Information System" means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.304.

H. “Medical Information” means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment and shall have the meaning given to such term under California Civil Code § 56.05.

I. “PHI” means Protected Health Information and Medical Information, collectively.

J. “Protected Health Information" means any information, including Electronic PHI, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including, but not limited to 45 CFR § 160.103. For the purposes of this Appendix, Protected Health Information includes all medical information and health insurance information as defined in California Civil Code § 1798.82.

K. “Secretary” means the Secretary, Department of Health and Human Services, or his or her designee.

L. "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, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.304.

M. “UC’s PHI” means any PHI that Supplier acquires, accesses, uses, discloses, modifies, or destroys in providing Goods and/or Services for UC.

N. “Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of an Encryption or Destruction technology or methodology specified by the Secretary in guidance issued under Section 13402(h)(2) of the HITECH Act on the Health and Human Services Web site, as such guidance may be revised from time to time, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.402.

ARTICLE 3 –SUPPLIER’S RESPONSIBILITIES

A. Permitted Uses and Disclosures of PHI. Supplier may use, access and/or disclose PHI received by Supplier pursuant to the Agreement between Supplier and UC, but only for the purpose of providing the Goods and/or Services required of Supplier by the Agreement or as otherwise required by law. Supplier may not

use, access and/or disclose PHI in any manner that would violate HIPAA if done by UC; except that (i) Supplier may use PHI for Supplier's proper management and administration, if necessary and subject to the requirements in Article 3.B herein, and (ii) Supplier may use PHI to provide data aggregation services relating to the health care operations of UC if expressly provided for in the Agreement. To the extent Supplier carries out one or more of UC's obligations under Subpart E of 45 CFR Part 164, Supplier must comply with the requirements of Subpart E that apply to UC in the performance of such obligation(s).

1. Minimum Necessary. With respect to the use, access, or disclosure of PHI by Supplier as permitted pursuant to this Appendix or the Agreement, Supplier shall limit such use access, or disclosure, to the Minimum Necessary to accomplish the intended purpose of such use, access, or disclosure. Supplier shall determine what constitutes the Minimum Necessary to accomplish the intended purpose in accordance with HIPAA, the HIPAA Regulations and any applicable guidance issued by the Secretary.

2. Documentation of Disclosures. With respect to any disclosures of UC'S PHI by Supplier as permitted under this Article 3, Supplier shall document such disclosures including, but not limited to, the date of the disclosure, the name and, if known, the address of the recipient of the disclosure, a brief description of the PHI disclosed, and a brief description of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure. Notwithstanding any record retention requirements elsewhere in the Agreement, for each disclosure of UC'S PHI, Supplier agrees to retain this accounting for a period of at least six (6) years from the date of such disclosure.

3. Electronic Transaction Standards. Where applicable, Supplier shall adhere to the transaction standards as specified in 45 CFR Parts 160 and 162.

B. Other Permitted Uses and Disclosures of PHI. Subject to the limitation in Article 3.C below, Supplier may, if necessary and only to the extent necessary, use, access or disclose PHI (i) for Supplier's proper management and administration, or (ii) to carry out Supplier's legal responsibilities. Supplier shall obtain reasonable assurances from the person to whom PHI is being disclosed that, as required under this Appendix, the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed. Supplier shall require that any Breaches or Security Incidents be immediately reported to Supplier. Supplier shall then report the Breach or Security Incident to UC in accordance with Article 3.G.

C. Nondisclosure of PHI. Supplier is not authorized and shall not use, access or further disclose UC's PHI other than as permitted or required under the Agreement, including this Appendix, or as required by law or regulation.

1. Disclosures Required by Law. In the event Supplier is or may be required by law to disclose PHI, including, but not limited to, pursuant to service with legal process or a request from a governmental agency, Supplier shall promptly notify UC of such requirement, and in any case, within five (5) business days of its receipt of such legal process or request. Supplier shall give UC reasonable opportunity to oppose such disclosure or take other appropriate action before Supplier discloses the PHI.

2. UC Consent Required. Supplier shall not disclose PHI without UC's consent unless pursuant to a valid and specific court order or to comply with a requirement for review of documents by a governmental regulatory agency under its statutory or regulatory authority to regulate the activities of either party.

D. Prohibition on Sale of PHI for Remuneration. Subject to the limitations set forth in 45 CFR § 164.502, Supplier shall not directly or indirectly receive remuneration in exchange for any of UC's PHI unless Supplier first obtains authorization from UC.

E. Security Standards. Supplier shall take appropriate security measures (i) to protect the confidentiality, integrity and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of UC and (ii) to prevent any use or disclosure of the PHI other than as provided by the Agreement and this

Appendix. Appropriate security measures include the implementation of the administrative, physical and technical safeguards specified in Subpart C of 45 CFR Part 164 of the HIPAA Security Rule.

F. Security Documentation. Supplier shall maintain the policies and procedures implemented to comply with Article 3.E in written form (paper or electronic). If an action, activity or assessment is required to be documented, Supplier shall maintain a written record (paper or electronic) of the action, activity, or assessment, shall retain the documentation for six (6) years from the date of its creation or the date when it last was in effect, whichever is later, make documentation available to those persons responsible for implementing the procedures to which the documentation pertains, and review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the PHI.

G. Notification of Breaches and Security Incidents. Supplier shall notify UC in writing as soon as possible, but in no event more than ten (10) business days, after Supplier becomes aware of any Breach or Security Incident involving UC's PHI. Supplier shall be deemed to be aware of any Breach or Security Incident as of the first day on which such Breach or Security Incident is known or reasonably should have been known to its officers, employees, agents or sub-suppliers. Supplier shall identify as soon as practicable each individual whose unsecured PHI has been, or is reasonably believed by Supplier to have been, accessed, acquired, or disclosed during such Breach or Security Incident. Supplier shall cooperate in good faith with UC in the investigation of any Breach or Security Incident. For purposes of this Appendix, the Parties agree that UC is on continued notice of the general pings and other routine attempted unauthorized accesses to Supplier's system and there is no need for further notification under this Appendix.

H. Prompt Corrective Actions. In addition to the notification requirements in Article 3.G, and with prior notice to UC, Supplier shall take (i) prompt corrective action to remedy any Breach or Security Incident, (ii) mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by Supplier, and (iii) take any other action required by applicable federal and state laws and regulations pertaining to such Breach or Security Incident.

1. Notification of Corrective Action and Provision of Policies. As soon as possible, but no later than fifteen (15) calendar days after discovery of the Breach or Security Incident, Supplier shall provide written notice to UC of (i) the actions initiated by Supplier to mitigate any harmful effect of such Breach or Security Incident and (ii) the corrective action Supplier has initiated or plans to initiate to prevent future similar Breaches or Security Incidents. UC shall have the right to make recommendations to Supplier regarding its corrective action, and Supplier shall reasonably consider, and work with UC, to implement such recommendations. Upon UC's request, Supplier will also provide to UC a copy of Supplier's policies and procedures that pertain to the Breach or Security Incident involving UC's PHI, including procedures for curing any material breach of this Appendix.

I. Use and Disclosure of De-Identified UC Data by Supplier. Supplier may only use or disclose UC de-identified data only if the de-identified data meets the standard and implementation specifications for de-identification under 45 CFR **§** 164.514 and (i) such use or disclosure is provided for in the Agreement or (ii) Supplier receives UC's prior written consent.

J. Supplier's Obligation to Provide Materials. Supplier shall make certain relevant information concerning the use, disclosure, or security of UC's PHI available to UC upon UC's request with the following restrictions. Supplier shall make its internal practices, books, and records relating to the use, disclosure, or security of UC's PHI available to any state or federal agency, including the U.S. Department of Health and Human Services, for purposes of determining UC's and/or Supplier's compliance with federal and state privacy and security laws and regulations.

L. Right to Review Supplier's Processes. UC has the right, at its discretion, to review facilities, systems, procedures, records, books, agreements, policies and procedures relating to the use and/or disclosure of UC's PHI to determine Supplier's compliance with federal and state privacy and security laws and

regulations. Except in the instance UC has received credible information of a Breach or Security Incident involving Supplier and UC's PHI, UC agrees to provide at least thirty (30) days' notice via a written request of its intent to review Supplier's processes and Supplier shall make available to UC and its authorized agents, during normal business hours, all facilities, systems, procedures, records, books, agreements, policies and procedure.

M. Supplier is required to disclose PHI (i) to the Secretary when required to investigate or determine UC's compliance with HIPAA, and (ii) to UC, the individual, or the individual's designee, as necessary to satisfy UC's obligations under 45 CFR 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of PHI.

N. Regulatory Compliance. In connection with all matters related to the Agreement and this Appendix, Supplier (i) acknowledges that it may not use or disclose PHI in a manner that would violate the requirements of federal or state law if done by UC, and (ii) shall comply with all applicable federal and state laws and regulations, including, but not limited to HIPAA; the HIPAA Regulations; 45 CFR §§ Parts 160, 162, and 164; the HITECH Act, Subtitle D, part 1; California Civil Code § 1798.29 and California Health and Safety Code § 1280.15, as they may be amended from time to time.

ARTICLE 4 - Parties' Responsibilities with Respect to Rights of Individuals

A. Individual's Right to Request Restrictions of PHI. If an individual or his or her representative requests that Supplier restrict the use and disclosure of the individual's PHI, Supplier shall notify UC in writing within five (5) business days after receipt of any request. Upon written notice from UC that it agrees to comply with the requested restrictions, Supplier agrees to comply with any instructions to modify, delete, or otherwise restrict the use and disclosure of the subject's PHI.

B. Individual's Request for Amendment of PHI. If the Agreement provides that an individual may request Supplier to amend the individual's PHI, Supplier shall inform UC within five (5) business days after receipt of any request by or on behalf of the subject of the PHI to amend the PHI that Supplier maintains for or on behalf of UC. Supplier shall, within twenty (20) calendar days after receipt of a written request, make the subject's PHI available to UC as may be required to fulfill UC's obligations to amend PHI pursuant to HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR § 164.526. Supplier shall, as directed by UC, incorporate any amendments to UC's PHI into copies of such PHI maintained by Supplier.

C. Individual's Request for an Accounting of Disclosures of PHI. If the Agreement provides that an individual may request an accounting of disclosures of the individual's PHI, Supplier shall document all disclosures of PHI and, within twenty (20) calendar days after receipt of a written request, make available to UC, and, if authorized in writing by UC, to the subject of the PHI, such information maintained by Supplier or its agents as may be required to fulfill UC's obligations to provide an accounting for disclosures of UC's PHI pursuant to HIPAA, the HIPAA Regulations, including, but not limited to, 45 CFR § 164.528, and the HITECH Act, including, but not limited to Section 13405(c).

D. Access to Certain Information in Electronic Format. If the Agreement provides that Supplier will use or maintain Electronic Health Records with respect to PHI on behalf of UC, Supplier shall, upon request of UC, provide UC with the requested Electronic Health Record in an electronic format.

ARTICLE 5 – Agents

A. In accordance with 45 CFR § 164.502(e)(1)(ii), to the extent Supplier contracts with Agents in the provision of Goods and/or Services pursuant to the Agreement, Supplier agrees that such Agents may create, receive, maintain or transmit PHI solely for the purpose of providing Goods and/or Services provided for in the Agreement.

B. Supplier shall require all Agents agree to the same restrictions and conditions that are imposed on Supplier by this Appendix, and to provide written assurance of such agreement, including, but not limited to, Articles 3.E (Security Standards), 3.F (Security Documentation) and 3.G (Notification of Breaches and Security Incidents).

ARTICLE 6 – TERMINATION AND OTHER REMEDIES

A. Material Breach. If UC determines that Supplier has violated a material term of this Appendix, UC may take any of the following actions, at its option:

1. Terminate all applicable agreements, including this Appendix, immediately.

2. Provide Supplier with notification of termination of the applicable agreements, including the Agreement and this Appendix, unless Supplier, within five (5) business days, provides a plan to cure the breach and, within fifteen (15) business days, cures the breach.

3. If termination is not feasible, upon UC's request, Supplier shall:

(a) at its expense, provide a third-party review of the outcome of any plan implemented under Article 6.A.2. to cure the breach; or

(b) at its expense, submit to a plan of monitoring and reporting to demonstrate compliance with this Appendix.

B. Effect of Termination: Return and/or Destruction of PHI held by Supplier or its Agents. Upon termination, expiration or other conclusion of the Appendix for any reason, Supplier shall return or, at UC's option, provide for the Destruction of all of UC's PHI, that Supplier and/or its Agents and sub-suppliers still maintain in any form, and shall retain no copies of UC's PHI. Within thirty (30) calendar days after the termination of this Appendix, Supplier shall both complete such return and/or Destruction and certify in writing to UC that such return or Destruction has been completed.

C. Return or Destruction Not Feasible. If Supplier represents to UC that return or Destruction of UC's PHI is not feasible, Supplier must provide UC with a written statement of the reason that return or Destruction by Supplier or its Agents is not feasible. If UC determines that return or Destruction is not feasible, this Appendix shall remain in full force and effect and shall be applicable to any and all of UC's PHI held by Supplier or its Agents.

ARTICLE 7 – CHANGES TO THIS APPENDIX

A. Compliance with Law. The parties acknowledge that state and federal laws and regulations relating to electronic data security and privacy are rapidly evolving and that additional obligations and responsibilities may be imposed on Supplier to ensure compliance with the new laws and regulations. The parties specifically agree to comply with all applicable laws and regulations and take such action as may be necessary to implement the standards and requirements of HIPAA, the HIPAA Regulations, the HITECH Act, and other applicable state and federal laws and regulations relating to the security or confidentiality of PHI, without need to amend or modify this Appendix. UC will update this Appendix from time to time as required by applicable laws and regulations, and Supplier agrees to sign a revised Appendix upon UC's reasonable request.

ARTICLE 8 – MISCELLANEOUS PROVISIONS

A. Assistance in Litigation or Administrative Proceedings. Supplier shall make itself, and any employees or

Agents assisting Supplier in the performance of its obligations under the Agreement or this Appendix, available to UC at no cost to UC to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings against UC, its directors, officers, agents or employees based upon claimed violation of HIPAA, the HIPAA Regulations or other laws relating to PHI security and privacy.

B. Order of Precedence. To the extent that the terms of any other agreement(s) between UC and Supplier are inconsistent with the terms of this Appendix, the terms of this Appendix will control.

C. Survival. The obligations of Supplier under Articles 3.A, 3.C**,** 3.D**,** 3.E, 3.F**,** 3.G, 3.H, 3.I, 3.J, 3.L, 3.M, 4.A, 4.D, 5.A, 7.A, 8.A, and 8.B of this Appendix shall survive the termination of any agreement between UC and Supplier.

The Appendix is signed below by the parties' duly authorized representatives.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA	**SUPPLIER**
	_____ (Supplier Name)
_____ (Signature)	_____ (Signature)
_____ (Printed Name, Title)	_____ (Printed Name, Title)
_____ (Date)	_____ (Date)