CSU The California State University

HIPAA Privacy and Business Associate Agreement

This Agreement is entered into this _____ day of _____, _____, between [*Employer*] ("Employer"), acting on behalf of [*Name of covered entity/plan(s) for which vendor provides services*] (the "Plan(s)"), and [*Name of vendor*] ("Business Associate"). The Agreement is incorporated into the [*Name of vendor contract*] between Employer and Business Associate, dated [*Date of Contract*] (the "Contract"). The parties intend to use this Agreement to satisfy the Business Associate contract requirements in the regulations at 45 CFR 164.502(e), 164.504(e) and 164.314(a), issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5) and regulations promulgated thereunder; and for further applicable HIPAA developments published after enactment of P.L. 111-5, including statutes, case law, regulations and other agency guidance. [*If there is no existing applicable vendor agreement, then this agreement will be a letter agreement between employer and the vendor*.]

1.0 Definitions

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 CFR part 160 and part 164, including sections 160.103, 164.103, 164.304 and 164.501. Notwithstanding the above, "Covered Entity" shall mean the [*Name of covered entity/plan*]; "Individual" shall mean the person who is the subject of the Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g); Protected Health Information shall have the meaning defined in 45 CFR.160.103, which also sets forth the definition of health information, including genetic information as clarified by P.L. 110-233 and applicable regulations; "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his designee; "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E; and "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information at 45 CFR part 160 and part 164, subparts A and C.

2.0 Obligations and activities of Business Associate

Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by Section 3.0 of this Agreement, or as required by law.

(a) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

(b) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(c) Business Associate agrees to report to Covered Entity, in writing, any use or disclosure of the Protected Health Information not provided for by this Agreement and any security incident of which it becomes aware. For purposes of this Agreement, security incident" shall have the same meaning as the term "security incident" in 45 CFR 164.304

(d) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information or electronic Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(e) Business Associate agrees to provide access, at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations, to Protected Health Information in a designated record set, to the Covered Entity or directly to an Individual in order to meet the requirements under 45 CFR 164.524.

(f) Business Associate agrees to make any amendment(s) to Protected Health Information in a designated record set that the Covered Entity or an Individual directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations.

(g) Business Associate 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 Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity, to the Secretary in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(h) Business Associate agrees to document disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(i) Business Associate agrees to provide to Covered Entity or an Individual an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528, in a prompt and reasonable manner consistent with the HIPAA regulations.

(j) Business Associate agrees to satisfy all applicable provisions of HIPAA standards for electronic transactions and code sets, also known as the Electronic Data Interchange (EDI) Standards, at 45 CFR Part 162. Business Associate further agrees to ensure that any agent, including a subcontractor that conducts standard transactions on its behalf will comply with the EDI Standards.

(k) Business Associate agrees to determine the minimum necessary type and amount of PHI required to perform its services and will comply with 45 CFR 164.502(b) and 514(d).

(l) Business Associate agrees to restrict the use or disclosure of Protected Health Information, and document those restrictions, at the request of Covered Entity pursuant to 45 CFR 164.522(a), in a prompt and reasonable manner consistent with the HIPAA regulations.

(m) Business Associate agrees to accommodate alternative means or alternative locations to communicate Protected Health Information, and document those alternative means or alternative locations, at the request of Covered Entity or an Individual, pursuant to 45 CFR 164.522(b), in a prompt and reasonable manner consistent with the HIPAA regulations.

(n) Business Associate agrees to be the primary party responsible for receiving and resolving requests from an Individual exercising his or her individual rights described in subsections (f), (g), (j), and (n) of this section 2.0.

(o) Business Associate agrees to implement any and all administrative, technical and physical safeguards necessary to reasonably and appropriately protect the confidentiality, integrity and availability of electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of the Plan(s).

(p) Business Associate agrees to ensure that access to electronic Protected Health Information related to the Covered Entity is limited to those workforce members who require such access because of their role or function.

(q) Business Associate agrees to implement safeguards to prevent its workforce members who are not authorized to have access to such electronic Protected Health Information from obtaining access and to otherwise ensure compliance by its workforce with the Security Rule.

(r) Business Associate acknowledges that enactment of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5, ARRA) amended certain provisions of HIPAA in ways that now directly regulate, or will on future dates directly regulate, Business Associate's obligations and activities under HIPAA's Privacy Rule and Security Rule. Requirements applicable to Business Associate under Title XIII, Subtitle D of ARRA are hereby incorporated by reference into the Agreement, including provisions that would govern the Plan's action if the Business Associate undertakes that action on behalf of the Plan. Business Associate agrees to comply, as of the applicable effective dates of each such HIPAA obligation relevant to Business Associate, with the requirements imposed by ARRA, including monitoring federal guidance and regulations published thereunder and timely compliance with such guidance and regulations. In consequence of the foregoing direct regulation of Business Associate by HIPAA laws and regulations, notwithstanding any other provision of the Agreement, Business Associate further agrees to monitor HIPAA Privacy and Security requirements imposed by future laws and regulations, and to timely

comply with such requirements when acting for or on behalf of the Plan in its capacity as a Business Associate.

(s) Further, Business Associate agrees to timely undertake all activities associated with the duties of ARRA section 13402 (and related guidance) in the event that Business Associate (or its agent) experiences a breach of Covered Entity's Protected Health Information requiring notice to affected individuals and/or any other party. Business Associate agrees that Covered Entity will be given reasonable advance opportunity to review the proposed notice or other related communications to any individual or third party regarding the breach; Covered Entity may propose revised or additional content to the materials which will be given reasonable consideration by Business Associate (or its agent).

3.0 Permitted or required uses and disclosures by Business Associate

(a) **General use and disclosure.**

(i) Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Contract and in this Agreement, provided that such use or disclosure of Protected Health Information would not violate the Privacy Rule, including the minimum necessary requirement, if done by Covered Entity.

(ii) Business Associate shall share Protected Health Information as reasonably requested by Covered Entity with Covered Entity and the Centers for Medicare and Medicaid Services (CMS), and with their agents and any other parties permitted by CMS guidance (including CMS's FAQ #5482), where the Covered Entity is submitting to CMS the Protected Health Information required by 42 CFR 423.884 for Medicare's retiree drug subsidy program.

(iii) Business Associate shall share Protected Health Information as reasonably requested by Employer to carry out its responsibilities as plan administrator of the Plan(s), including, without limitation, for purposes of auditing the performance of Business Associate.

(b) **Additional use and disclosure.**

(i) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(ii) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that such disclosures are required by law, or Business

Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be 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 Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(iii) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide data aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).

(iv) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

4.0 Obligation to inform Business Associate of Covered Entity's privacy practices and any authorization or restriction

(a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, authorization by Individual or his or her personal representative to use or disclose Protected Health Information, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

5.0 Permissible requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

6.0 Term and termination

(a) **Term.** The term of this Agreement shall be effective as of _____ [*date on or after April 20, 2005 – there may be a different date depending on the effective date of the EAP contract*]**,** and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to 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.** The Covered Entity may, in its sole discretion, provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Contract if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate the Contract if Business Associate has breached a material term of this Agreement and cure is not possible. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary of Health and Human Services.

(c) **Effect of termination.** The parties mutually agree that it is essential for Protected Health Information to be maintained after the expiration of the Agreement for regulatory and other business reasons. The parties further agree that it would be infeasible for Covered Entity to maintain such records because Covered Entity lacks the necessary system and expertise. Accordingly, Covered Entity hereby appoints Business Associate as its custodian for the safe keeping of any record containing Protected Health Information that Business Associate may determine it is appropriate to retain. Notwithstanding the expiration or termination of the Contract, Business Associate shall extend the protections of this Agreement to such Protected Health Information, and limit further use or disclosure of the Protected Health Information to those purposes that make the return or destruction of the Protected Health Information infeasible.

7.0 Miscellaneous

(a) **Regulatory references.** A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended, and for which compliance is required.

(b) **Amendment.** Upon the enactment of any law or regulation affecting the use, disclosure, or safeguarding of Protected Health Information or electronic Protected Health Information, or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either party may, by written notice to the other party, amend the Contract and this Agreement in such manner as such party determines necessary to comply with such law or regulation. If the other party disagrees with such amendment, it shall so notify the first party in writing within thirty (30) days of the notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, then either of the parties may terminate the Contract on thirty (30) days written notice to the other party.

(c) **Survival.** The respective rights and obligations of Business Associate under Section 6.0 of this Agreement shall survive the termination of this Agreement.

(d) **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy and Security Rules.

(e) **No third party beneficiary.** Nothing expressed or implied in this Agreement or in the Contract is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assignees of the parties, any rights, remedies, obligations, or liabilities whatsoever.

(f) **Severability.** If any provision of this Agreement is held illegal, invalid, prohibited or unenforceable by a court of competent jurisdiction, that provision shall be limited or eliminated in that jurisdiction to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.

(g) **Governing law.** This Agreement shall be governed by and construed in accordance with the laws of the state of California to the extent not preempted by the Privacy or Security Rules or other applicable federal law.

(h) **Indemnification and performance guarantees.** The indemnification and performance guarantee provisions contained in the Contract shall also apply to this Agreement.

[*For Employer*]	[*For Vendor*]
By:_____	By:_____
Name: _____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____