Exhibit __ [Insert alpha letter]
UC HIPAA Business Associate Addendum

Revised 1/08 by Roberta Ward and approved by UC. Exhibit use instructions appear in CMU Notice 07-01. No alterations to this exhibit including margins, font size, and content are allowed without prior DHCS OLS approval. Remove these shaded instructions before use.

I. Recitals

A. This Contract (Agreement) has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act ("HIPAA") and its implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations:").

B. The Department of Health Care Services ("DHCS") wishes to disclose to Business Associate certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI").

C. "Protected Health Information" or "PHI" shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended from time to time, and that is created, maintained or received by Contractor on behalf of DHCS.

D. "Security Incident" shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended from time to time.

E. As set forth in this Agreement, Contractor, the University of California, here and after, is the Business Associate of DHCS that provides services, arranges, performs or assists in the performance of functions or activities on behalf of DHCS and creates, receives, maintains, transmits, uses or discloses PHI.

F. DHCS and Business Associate desire to protect the privacy and provide for the security of PHI created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, in compliance with HIPAA and HIPAA regulations and other applicable laws.

G. The purpose of the Addendum is to satisfy certain standards and requirements of HIPAA and the HIPAA regulations.

H. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms in the HIPAA regulations.

In exchanging information pursuant to this Agreement, the parties agree as follows:

1. Permitted Uses and Disclosures of PHI by Business Associate

A. ***Permitted Uses and Disclosures.*** Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of DHCS, provided that such use or disclosure would not violate the HIPAA regulations, if done by DHCS.

B. ***Specific Use and Disclosure Provisions.*** Except as otherwise indicated in this Addendum, Business Associate may:

1) ***Use and disclose for management and administration.*** Use and disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or the Business Associate

obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will 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 that the confidentiality of the information has been breached.

2) ***Provision of Data Aggregation Services.*** Use PHI to provide data aggregation services to DHCS. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of DHCS with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of DHCS.

2. Responsibilities of Business Associate

Business Associate agrees:

A. ***Nondisclosure.*** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by this Agreement or as required by law.

B. ***Safeguards.*** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of DHCS; and to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate shall develop and maintain an information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities, and which incorporates the requirements of section C, Security, below. Business Associate will provide DHCS with its current and updated policies upon request.

C. ***Security.*** To take any and all reasonable and appropriate steps to ensure the security of all computerized data systems containing PHI, and provide data security procedures for the use of DHCS at the end of the contract period. These steps shall include, at a minimum:

1) Complying with all of the data system security precautions listed in this Agreement and in the Attachment A portion of this Addendum;

2) Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement;

3) Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III-Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

4) In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of this Agreement.

Business Associate shall designate a Security Officer for each campus to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with DHCS.

Exhibit __ [Insert alpha letter]
UC HIPAA Business Associate Addendum

D. ***Mitigation of Harmful Effects***. To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

E. ***Business Associate's Agents***. To ensure that any agents, including subcontractors, to whom Business Associate provides PHI received from or created or received by Business Associate on behalf of DHCS, agree to the same restrictions and conditions that apply to Business Associate with respect to such PHI, including implementation of reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI; and to incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or subaward to such agents or subcontractors.

F. ***Availability of Information to DHCS and Individuals***. If Business Associate creates or maintains the Designated Record Set on behalf of DHCS, Business Associate will provide access as DHCS may require, and in the time and manner designated by DHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to DHCS (or, as directed by DHCS), to an Individual, in accordance with 45 CFR Section 164.524. Designated Record Set means the group of records maintained by Business Associate for DHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DHCS health plans; or those records used to make decisions about individuals on behalf of DHCS. Business Associate shall use the forms and processes developed and provided by DHCS for this purpose and shall respond to requests for access to records transmitted by DHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

G. ***Amendment of PHI***. To make any amendment(s) to PHI that DHCS directs or agrees to pursuant to 45 CFR Section 164.526, in the time and manner designated in writing by DHCS.

H. ***Internal Practices***. To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from DHCS, or created or received by Business Associate on behalf of DHCS, available to DHCS or to the Secretary of the U.S. Department of Health and Human Services, for purposes of determining DHCS' compliance with the HIPAA regulations.

I. ***Documentation of Disclosures***. To document and make available to DHCS or (at the direction of DHCS) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with 45 CFR 164.528.

J. ***Notification of Breach***. During the term of this Agreement:

1) ***Discovery of Breach***. To notify DHCS **immediately by telephone call plus email or fax** upon the discovery of breach of security of PHI in computerized form if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person; or **within 24 hours by email or fax** of the discovery of any security incident or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or loss of confidential data affecting this Agreement. Notification shall be provided to the DHCS Privacy Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notification shall be provided by calling the DHCS ITSD Help Desk. Business Associate shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and

ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

2) ***Investigation of Breach.*** To immediately investigate such security incident, breach, or unauthorized use or disclosure of PHI. Within 72 hours of the discovery, to notify the DHCS Privacy Officer of, to the extent known to the Business Associate:

i. What data elements were involved and the extent of the data involved in the breach,
ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI,
iii. A description of where the PHI is believed to have been improperly transmitted, sent, or utilized,
iv. A description of the probable causes of the improper use or disclosure; and
v. Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered.

Business Associate shall notify the DHCS Privacy Officer immediately when Business Associate becomes aware of additional material information.

3) ***Written Report.*** To provide a written report of the status of the investigation to the DHCS Privacy Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. To the extent information is known to the Business Associate, the report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

4) ***Notification of Individuals.*** To notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and to pay any costs of such notifications. The DHCS Privacy Officer and Business Associate shall determine the time, manner and content of any such notifications.

5) ***DHCS Contact Information.*** To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated herein. DHCS reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or Addendum.

DHCS Contract Manager	**DHCS Privacy Officer**	**DHCS Information Security Officer**
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer c/o: Office of Legal Services Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Help Desk (916) 440-7000 or (800) 579-0874

K. ***Workforce Training and Discipline.*** To train and use reasonable measures to provide for compliance with the requirements of this Addendum by workforce members who assist in the performance of functions or activities on behalf of DHCS under this Agreement and use or disclose PHI; and discipline such workforce members who intentionally violate any provisions of this Addendum, with possible

sanctions to include termination of employment. In complying with the provisions of this section, Business Associate shall observe the following requirements:

1) Business Associate shall provide information privacy and security training, at least annually, at its own expense, to all its workforce members who assist in the performance of functions or activities on behalf of DHCS under this Agreement and use or disclose PHI.

2) Business Associate shall require each workforce member who receives information privacy and security training to sign a certification, indicating the workforce members' name and the date on which the training was completed.

3) Business Associate shall retain each workforce member's written certifications for DHCS inspection for a period of three years following contract termination.

3. Obligations of DHCS

DHCS agrees to:

A. ***Notice of Privacy Practices***. Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR 164.520, as well as any changes to such notice. Visit this Internet address to view the most current Notice of Privacy Practices: http://www.dhs.ca.gov/privacyoffice.

B. ***Permission by Individuals for Use and Disclosure of PHI***. Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.

C. ***Notification of Restrictions***. Notify the Business Associate of any restriction to the use or disclosure of PHI that DHCS has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

D. ***Requests Conflicting with HIPAA Rules***. Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations if done by DHCS.

4. Audits, Inspection and Enforcement

From time to time and with reasonable notice and during normal business hours, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the DHCS Privacy Officer in writing. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does DHCS':

A. Failure to detect or

B. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of DHCS' enforcement rights under this Agreement and this Addendum.

5. Termination

Exhibit __ [Insert alpha letter]
UC HIPAA Business Associate Addendum

A. ***Termination for Cause***. Upon DHCS' knowledge of a material breach of this Addendum by Business Associate, DHCS shall:

1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within thirty days.;

2) Immediately terminate this Agreement if Business Associate has breached a material term of this Addendum and cure is not possible; or

3) If neither cure nor termination is feasible, report the violation to the Secretary of the U.S. Department of Health and Human Services.

B. ***Judicial or Administrative Proceedings***. Business Associate will notify DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. DHCS may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA.

C. ***Effect of Termination***. Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from DHCS (or created or received by Business Associate on behalf of DHCS) that Business Associate still maintains in any form, and shall retain no copies of such PHI or, if return or destruction is not feasible, shall continue to extend the protections of this Addendum to such information, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

6. Miscellaneous Provisions

A. ***Disclaimer***. DHCS makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

B. ***Amendment***. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon DHCS' request, Business Associate agrees to promptly enter into negotiations with DHCS concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HIPAA regulations or other applicable laws. DHCS may terminate this Agreement upon thirty (30) days written notice in the event:

1) Business Associate does not promptly enter into negotiations to amend this Addendum when requested by DHCS pursuant to this Section or

2) Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that DHCS reasonably deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

Exhibit __ [Insert alpha letter]
UC HIPAA Business Associate Addendum

C. ***Assistance in Litigation or Administrative Proceedings***. Business Associate and DHCS shall each make itself and use its best efforts to make any subcontractors, employees or agents assisting it in the performance of its obligations under this Agreement, available to the other party at no cost to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against either party, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by DHCS or the Business Associate, except where the party or its subcontractor, employee or agent is a named adverse party.

D. ***No Third-Party Beneficiaries***. Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than DHCS or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

E. ***Interpretation***. The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA regulations.

F. ***Regulatory References***. A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.

G. ***Survival***. The respective rights and obligations of Business Associate under Section 6.C of this Addendum shall survive the termination or expiration of this Agreement.

H. ***No Waiver of Obligations***. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

Exhibit __ [Insert alpha letter]
UC HIPAA Business Associate Addendum

Attachment A
Business Associate Data Security Requirements

1. General Security Controls

A. ***Confidentiality Training***. All persons that will be working with DHCS data must be trained on General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies.

B. ***Background check.*** Before a member of the Contractor's workforce may access DHCS data, Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data.

C. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store DHCS data must be encrypted with a University of California approved solution comparable to ones available to the state through the California Strategic Sourced Initiative (CSSI).

D. Only the minimum necessary amount of DHCS data may be downloaded to a laptop or hard drive when absolutely necessary for business purposes.

E. ***Removable media devices.*** All electronic files that contain DHCS data must be encrypted when stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, etc.) with a University of California approved solution which is comparable to a solution using a CSSI vendor product.

F. ***Email security.*** All emails that include DHCS data must be sent in an encrypted method using a University of California approved solution which is comparable to a solution using a CSSI vendor product.

G. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store DHCS data must have a commercial third-party anti-virus software solution with a minimum daily automatic update.

H. ***Patch Management.*** All workstations, laptops and other systems that process and/or store DHCS data must have security patches applied.

I. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DHCS data. Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed every 60 days. Must be changed if revealed or compromised. Must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

J. ***Data Destruction.*** All DHCS data must be wiped from systems when the data is no longer necessary. The wipe method must conform to Department of Defense standards for data destruction. All DHCS data on removable media must be returned to DHCS when the data is no longer necessary. Once data has been destroyed, the DHCS contract manager must be notified.

Exhibit __ [Insert alpha letter]
UC HIPAA Business Associate Addendum

Attachment A
Business Associate Data Security Requirements

K. ***Remote Access.*** Any remote access to DHCS PHI must be executed over an encrypted method approved by the University of California which is comparable to a solution using a CSSI vendor product. All remote access must be limited to minimum necessary and least privilege principles.

2. System Security Controls

A. ***System Timeout.*** The system must provide an automatic timeout after no more than 20 minutes of inactivity.

B. ***Warning Banners.*** All systems containing DHCS PHI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

C. ***System Logging.*** The system must log success and failures of user authentication at all layers. The system must log all system administrator/developer access and changes if the system is processing and/or storing PHI. The system must log all user transactions at the database layer if processing and/or storing DHCS PHI.

D. ***Access Controls.*** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.

E. ***Transmission encryption.*** All data transmissions must be encrypted end-to-end using a University of California approved solution, which is comparable to a solution using a CSSI vendor product, when processing and/or storing DHCS PHI.

F. ***Host Based Intrusion Detection.*** All systems that are accessible via the Internet or store DHCS PHI must have a suitable intrusion detection and prevention program.

3. Audit Controls

A. ***System Security Review.*** All systems processing and/or storing DHCS PHI must have at least an annual system security review. Reviews must include administrative and technical vulnerability scanning tools.

B. ***Log Reviews.*** All systems processing and/or storing DHCS PHI must have a routine procedure in place to review system logs for unauthorized access. Logs must be maintained for six years after the occurrence.

C. ***Change Control.*** All systems processing and/or storing DHCS PHI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity / Disaster Recovery Controls

A. ***Emergency Mode Operation Plan.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS PHI in the event of an emergency.

Exhibit __ [Insert alpha letter]
UC HIPAA Business Associate Addendum

Attachment A
Business Associate Data Security Requirements

B. ***Data Backup Plan.*** Contractor must have established documented procedures to backup DHCS data to maintain retrievable exact copies of DHCS PHI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup tapes, the amount of time to restore DHCS data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

5. Paper Document Controls

A. ***Supervision of Data.*** DHCS PHI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. ***Visitors.*** DHCS PHI shall be kept out of sight while visitors are in the area.

C. ***Confidential Destruction.*** DHCS PHI must be disposed of through confidential means, such as shredding and pulverizing.

D. ***Removal of Data.*** DHCS PHI must not be removed from the premises of the Contractor except with express permission of DHCS.

E. ***Faxing.*** Faxes containing DHCS PHI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified before sending.

F. ***Mailing.*** DHCS PHI shall only be mailed using secure methods. Large volume mailings of DHCS PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a University of California approved solution which is comparable to a solution using a CSSI vendor product.