

**Exhibit K**  
HIPAA Business Associate Addendum

**I. Recitals – HIGH RISK**

- 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 California Department of Public Health (“CDPH”) 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” means any information, whether oral or recorded in any form or medium that relates to the past, present, or future physical or mental condition of an individual, the provision of health and dental care to an individual, or the past, present, or future payment for the provision of health and dental care to an individual; and 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. PHI shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended from time to time.
- D. “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI, or confidential data that is essential to the ongoing operation of the Business Associate’s organization and intended for internal use; or interference with system operations in an information system.
- E. As set forth in this Agreement DHCS, here and after, is the Business Associate of CDPH that provides services, arranges, performs or assists in the performance of functions or activities on behalf of CDPH and creates, receives, maintains, transmits, uses or discloses PHI.
- F. CDPH 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 CDPH, provided that such use or disclosure would not violate the HIPAA regulations, if done by CDPH.

**Exhibit K**  
HIPAA Business Associate Addendum

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 CDPH. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of CDPH 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 CDPH.

**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 CDPH; and to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate shall develop and maintain a written 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 CDPH with its current and updated policies.
- C. **Security.** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI, and provide data security procedures for the use of CDPH 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 or in an Exhibit incorporated into this Agreement;
  - 2) Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of CDPH 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

**Exhibit K**  
HIPAA Business Associate Addendum

- 4) Complying with the safeguard provisions in the Department's Information Security Policy, embodied in Health Administrative Manual (HAM), sections 6-1000 et seq. and in the Security and Risk Management Policy in the Information Technology Section of the State Administrative Manual (SAM), sections 4840 et seq., in so far as the security standards in these manuals apply to Business Associate's operations. 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 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 CDPH.

- 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 CDPH, 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 CDPH and Individuals.** To provide access as CDPH may require, and in the time and manner designated by CDPH (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to CDPH (or, as directed by CDPH), to an Individual, in accordance with 45 CFR Section 164.524. Designated Record Set means the group of records maintained for CDPH that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for CDPH health plans; or those records used to make decisions about individuals on behalf of CDPH. Business Associate shall use the forms and processes developed by CDPH for this purpose and shall respond to requests for access to records transmitted by CDPH 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 CDPH directs or agrees to pursuant to 45 CFR Section 164.526, in the time and manner designated by CDPH.
- H. **Internal Practices.** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from CDPH, or created or received by Business Associate on behalf of CDPH, available to CDPH or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by CDPH or by the Secretary, for purposes of determining CDPH's compliance with the HIPAA regulations.
- I. **Documentation of Disclosures.** To document and make available to CDPH or (at the direction of CDPH) 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.

**Exhibit K**  
HIPAA Business Associate Addendum

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

- 1) **Discovery of Breach.** To notify CDPH **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 any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the CDPH contract manager, the CDPH Privacy Officer and the CDPH Information Security 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 CDPH 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 or confidential data. Within 72 hours of the discovery, to notify the CDPH contract manager(s), the CDPH Privacy Officer, and the CDPH Information Security Officer of:
  - 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 or confidential data,
  - iii. A description of where the PHI or confidential data 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.
- 3) **Written Report.** To provide a written report of the investigation to the CDPH contract managers, the CDPH Privacy Officer, and the CDPH Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. 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, as well as any costs associated with the breach. The CDPH contract manager, the CDPH Privacy Officer, and the CDPH Information Security Officer shall approve the time, manner and content of any such notifications.
- 5) **CDPH Contact Information.** To direct communications to the above referenced CDPH staff, the Contractor shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by giving written notice to the Department of Health Care Services. Said changes shall not require an amendment to this Agreement or Addendum.

**Exhibit K**  
HIPAA Business Associate Addendum

CDPH Contract Manager	CDPH Privacy Officer	CDPH Information Security Officer
See Exhibit A for 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: <a href="mailto:privacyofficer@dhs.ca.gov">privacyofficer@dhs.ca.gov</a> Telephone: (916) 445-4646	Information Security Officer Information Security Office P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413  Email: <a href="mailto:dhsiso@dhs.ca.gov">dhsiso@dhs.ca.gov</a> Telephone: ITSD Help Desk (916) 440-7000 or (800) 579-0874

K. **Employee Training and Discipline.** To train and use reasonable measures to ensure compliance with the requirements of this Addendum by employees who assist in the performance of functions or activities on behalf of CDPH under this Agreement and use or disclose PHI; and discipline such employees who intentionally violate any provisions of this Addendum, including by termination of employment. In complying with the provisions of this section K, 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 employees who assist in the performance of functions or activities on behalf of CDPH under this Agreement and use or disclose PHI.
- 2) Business Associate shall require each employee who receives information privacy and security training to sign a certification, indicating the employee's name and the date on which the training was completed.
- 3) Business Associate shall retain each employee's written certifications for CDPH inspection for a period of three years following contract termination.

**3. Obligations of CDPH**

CDPH agrees to:

- A. **Notice of Privacy Practices.** Provide Business Associate with the Notice of Privacy Practices that CDPH 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 CDPH 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 CDPH.

**Exhibit K**  
HIPAA Business Associate Addendum

**4. Audits, Inspection and Enforcement**

From time to time, CDPH 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 CDPH Privacy Officer in writing. The fact that CDPH 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 CDPH':

- 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 CDPH' enforcement rights under this Agreement and this Addendum.

**5. Termination**

- A. **Termination for Cause.** Upon CDPH' knowledge of a material breach of this Addendum by Business Associate, CDPH 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 the time specified by CDPH;
  - 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 CDPH if it is named as a defendant in a criminal proceeding for a violation of HIPAA. CDPH may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. CDPH may terminate this Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.
- C. **Effect of Termination.** Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from CDPH (or created or received by Business Associate on behalf of CDPH) 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.** CDPH 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

**Exhibit K**  
HIPAA Business Associate Addendum

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 CDPH' request, Business Associate agrees to promptly enter into negotiations with CDPH concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HIPAA regulations or other applicable laws. CDPH 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 CDPH pursuant to this Section or
  - 2) Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that CDPH in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.
- C. **Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, 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 the Business Associate, except where Business Associate 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 CDPH 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.