STATE OF CALIFORNIA
STANDARD AGREEMENT
STD 213 (Rev 06/03)

REGISTRATION NUMBER	AGREEMENT NUMBER
	13-20691

1. This Agreement is entered into between the State Agency and the Contractor named below:

STATE AGENCY'S NAME (Also referred to as CDPH or the State)
California Department of Public Health

CONTRACTOR'S NAME (Also referred to as Contractor)
Santa Barbara County Public Health Department

2. The term of this Agreement is: July 1, 2013 through June 30, 2016

3. The maximum amount of this Agreement is: $ 0 Zero Dollars

4. The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of this Agreement.

Exhibit A – Scope of Work	4 pages
Exhibit A-I – Definition of Terms	1 Page
Exhibit C * – General Terms and Conditions	GTC 610
Exhibit D – HIPAA Business Associate Exhibit	11 page

Items shown above with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.
These documents can be viewed at http://www.ols.dgs.ca.gov/Standard+Language.

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR

CONTRACTOR'S NAME *(if other than an individual, state whether a corporation, partnership, etc.)*
Santa Barbara County Public Health Department

BY *(Authorized Signature)* | DATE SIGNED *(Do not type)*

PRINTED NAME AND TITLE OF PERSON SIGNING

ADDRESS
300 N. San Antonio Drive, Santa Barbara, CA 93110

STATE OF CALIFORNIA

AGENCY NAME
California Department of Public Health

BY *(Authorized Signature)* | DATE SIGNED *(Do not type)*

PRINTED NAME AND TITLE OF PERSON SIGNING
Yolanda Murillo, Chief, Contracts Management Unit

ADDRESS
1616 Capitol Avenue, Suite 74.317, MS 1802, PO Box 997377
Sacramento, CA 95899-7377

California Department of General Services Use Only

[X] Exempt per: OOA Budget Act 2013

Exhibit A
Scope of Work

1. Service Overview

California Health and Safety Code 131019 designates the California Department of Public Health (CDPH), Center for Infectious Diseases, Office of AIDS (OA) as the lead agency within the state responsible for coordinating state programs, services and activities related to HIV and AIDS.

The Contractor agrees to provide CDPH/OA the services described herein.

2. Service Location

The services shall be performed at Santa Barbara County Public Health Department, including locations in Lompoc and Santa Maria, CA.

3. Project Representative

A. The project representatives during the term of this agreement will be:

California Department of Public Health Celia Banda-Brown, OA ADAP Chief Telephone: (916) 449-5943 Fax: (916) 449-5859 Email: Celia.Banda-Brown@cdph.ca.gov	**Agency Name: County of Santa Barbara** Site Contact: Graciela Prado Telephone: (805) 681-5463 Fax: (805) 681-5404 Email: graciela.prado@sbcphd.org

B. Direct all inquiries to:

California Department of Public Health OA ADAP Advisor Attention: Jessica Monasterio MS 7700, P.O. Box 997426 Sacramento, CA 95899-7426 Telephone: (916) 445-8493 Fax: (916) 449-5859 Email: Jessica.monasterio@cdph.ca.gov	**Agency Name: County of Santa Barbara** Attention: Takashi Wada, Director 300 N. San Antonio Drive Santa Barbara, CA 93110 Telephone: (805) 681-5105 Fax: (805) 681-5191 Email: takashi.wada@sdcphd.org

C. Either party may make changes to the information above by giving written notice to the other party. Said changes shall not require an amendment to this agreement.

4. Services to be Performed

1) Adhere to the ADAP "Enrollment Procedures and Guidelines for Determining ADAP Eligibility" and any subsequent revisions, along with all instructions, policy memorandums, or directives issued by the CDPH/OA, and/or the statewide ADAP PBM. The CDPH/OA will make any changes and/or additions to these guidelines in writing and, whenever possible, notification of such changes shall be made 30 days prior to implementation.

Exhibit A
Scope of Work

2) Designate an ADAP Enrollment Site contact to carry out the requirements of this contract agreement on behalf of the ADAP Enrollment Site and facilitate the following information exchange between CDPH/OA, the ADAP Coordinator, and the ADAP PBM:
   a. Notify the ADAP Coordinator and the ADAP PBM of any ADAP EW job duties or employment status changes that affect their status as an ADAP EW.
   b. Coordinate the activation of new ADAP EW identification (ID) numbers and de-activation of non-active ADAP EW ID numbers.
   c. Ensure ADAP EWs complete accurate ADAP client eligibility documentation for the initial enrollment and subsequent recertification, and adhere to ADAP eligibility guidelines and policies.
   d. Distribute CDPH/OA and/or ADAP PBM information to all ADAP EWs at the site.
   e. Notify the ADAP Coordinator of ADAP Enrollment Site concerns or problems, including any planned site relocation/change of address, upon discovery.
   f. Facilitate CDPH/OA site visit requests.

3) Ensure all ADAP EWs successfully complete training provided by the ADAP PBM prior to enrolling or re-certifying ADAP clients. All ADAP EWs must complete annual refresher trainings provided by the ADAP PBM to receive certification from the ADAP PBM in order to continue conducting ADAP enrollment functions.

4) Assure each ADAP EW at the site signs and submits to CDPH/OA the "Agreement by Employee/Contractor to Comply with Confidentiality Requirements (CDPH 8689)" on an annual basis. Submission of the form will be required at the time of mandatory ADAP EW recertification training. The ADAP EWs recertification process will not be complete until the completed form is received by CDPH/OA.

5) Ensure all ADAP EWs must be identified and have individual ADAP ID numbers issued by the ADAP PBM. This number may only be used by the EW to whom it was assigned. Enrollment of ADAP clients must be linked to individual ADAP EW ID numbers (i.e. to the specific enrollment worker performing the services at the specific Enrollment Site). EWs conducting ADAP enrollments/re-certifications at multiple ADAP Enrollment Sites must have an ADAP EW ID number unique to each CDPH/OA-approved ADAP Enrollment Site.

6) Report any changes in ADAP EW status (e.g. termination, relocation, separation, etc.) to the ADAP Coordinator and the ADAP PBM within 24 hours. Such reporting is required to assure termination of ADAP EW privileges, including access to ADAP client information, and to protect the confidentiality of the ADAP PBM database.

7) Ensure if an ADAP Enrollment Site chooses to enroll clients electronically through the ADAP PBM secure website, only desktop computers can be used. For purposes of security and to protect the confidentiality of ADAP client information, the use of laptop computers is prohibited for ADAP client enrollment purposes.

8) Notify the ADAP Coordinator, the ADAP PBM, and CDPH/OA if the site wishes to change from an open site (one which serves any individual who wishes to enroll) to a closed site (one which serves only agency-affiliated individuals) or vice versa. The ADAP Enrollment Site contact will notify all parties within 30 days prior to the change in status.

Exhibit A
Scope of Work

9) Ensure no ADAP EW is employed by nor receives any financial compensation, including gifts or any type of incentive, from a participating ADAP pharmacy.

10) ADAP client enrollment may not occur at a participating ADAP pharmacy location.

11) Maintain confidential client file records (electronic or hard copy) required to document ADAP client eligibility. These records are to be maintained separate and apart from any other client-related information at the site. Only authorized ADAP EWs can have access to ADAP client eligibility file information, unless otherwise authorized by law or the client. For purposes of federal audit requirements, client files/records shall be maintained for four years (the current year, plus three prior years).

12) Provide access to all ADAP client eligibility files and any other documentation related to this contract agreement. Access shall be granted during normal working hours to authorized representatives of CDPH/OA and other state and federal agencies, and are subject to applicable state and federal laws concerning confidentiality.

13) Ensure no client eligibility documentation, records, files, etc., will be transported to or from the ADAP Enrollment Site. Exception to this restriction may be approved by CDPH/OA for the following reasons:
    a. Client disability; or,
    b. Remote distance requires ADAP EW to meet with client outside of the ADAP Enrollment Site; or,
    c. The entire ADAP Enrollment Site is moving to a new address/location.

    Prior to transporting any ADAP client enrollment files, the site agrees to submit a written request to CDPH/OA which justifies the necessity for off-site client enrollment or identifies the relocation of the files to a new address/location. The request shall include a "Plan for Transporting Confidential ADAP Client Files", which identifies the specific procedure that will be followed to safeguard the confidentiality of the ADAP client documents being transported, as well as who will be responsible/accountable for this procedure. The site further agrees no client enrollment files will be transported until CDPH/OA provides written notification that the policies/procedures were deemed appropriate.

14) Ensure fax machines used to submit ADAP applications or receive ADAP correspondence which include confidential client information must be located in a secure area such that the confidentiality of the information sent and received is maintained at all times. The ADAP Enrollment Site must assure only certified ADAP EWs have access to confidential ADAP client information sent or received by fax.

15) Agree to the provisions as stated in Exhibit C, "NON-DISCRIMINATION CLAUSE." During the performance of this Agreement, Contractor and its subcontractors shall not unlawfully discriminate, harass, or allow harassment against any employee or applicant for employment because of sex, race, color, ancestry, religious creed, national origin, physical disability (including HIV and AIDS), mental disability, medical condition (e.g., cancer), age (over 40), marital status, and denial of family care leave.

Exhibit A
Scope of Work

16) Agree to the provisions as stated in Exhibit D, "Health Insurance Portability and Accountability Act (HIPAA) Business Associate Exhibit."

17) Arrange for the transfer/relocation of the ADAP client files through the ADAP Coordinator if an ADAP Enrollment Site ceases to conduct ADAP enrollment for any reason. Additionally, the ADAP Enrollment Site must notify CDPH/OA and the ADAP PBM of the planned deactivation of the site. Such reporting is necessary to assure termination of EW privileges, including access to ADAP client information, to protect the confidentiality of the ADAP PBM database, and to provide current and accurate ADAP Enrollment Site information to individuals wanting to access ADAP services statewide.

18) Make a copy of this contract agreement available to the ADAP EWs and agree to ensure they acknowledge and comply with the contents herein.

Exhibit A-1
Definition of Terms

CDPH/OA – Works collaboratively with state and federal agencies, local health jurisdictions, universities, and community-based organizations to ensure that efforts to combat the HIV/AIDS epidemic are targeted and effective.

AIDS Drug Assistance Program (ADAP) - Established in 1987 to help ensure that eligible, HIV-positive uninsured and under-insured individuals have access to HIV-related medication.

Local Health Jurisdiction (LHJ) – One of fifty-eight counties and three cities (Pasadena, Long Beach, and Berkeley) in the state of California.

Pharmacy Benefits Management (PBM) - Service contractor providing operational support for ADAP.

ADAP Coordinator - LHJ or other local agency staff designated to act as the primary county contact between the ADAP Enrollment Sites, the ADAP PBM, and CDPH/OA.

ADAP Enrollment Site - CDPH/OA-approved local site providing ADAP enrollment services for potentially eligible individuals.

ADAP Enrollment Worker (EW) – ADAP Enrollment Site staff trained by the ADAP PBM and certified to provide ADAP enrollment services.

OA/ADAP Advisor – OA/ADAP staff assigned to LHJ and ADAP Enrollment Sites for technical assistance.

Exhibit D
HIPAA Business Associate Exhibit

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 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") pursuant to HIPAA regulations.

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 Contractor 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.

G. The purpose of this Exhibit is to satisfy certain standards and requirements of HIPAA and the HIPAA regulations, and other applicable laws.

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

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

Exhibit D
HIPAA Business Associate Exhibit

II. Permitted Uses and Disclosures of PHI by Business Associate

A. ***Permitted Uses and Disclosures.*** Except as otherwise indicated in this Exhibit, 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.

B. ***Specific Use and Disclosure Provisions.*** Except as otherwise indicated in this Exhibit, 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.

III. 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.*** The Business Associate shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing CDPH PHI. These steps shall include, at a minimum:

1) complying with all of the data system security precautions listed in the Business Associate Data Security Standards set forth in Attachment 1 to this Exhibit;
2) 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 D
HIPAA Business Associate Exhibit

3) 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 CDPH PHI from breaches and security incidents.

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 Exhibit.

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 Exhibit 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 care component 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.

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 the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Exhibit, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information

Exhibit D
HIPAA Business Associate Exhibit

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 Program Contract Manager(s), the CDPH Privacy Officer, and the CDPH Chief 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 Program Contract Managers, the CDPH Privacy Officer, and the CDPH Chief 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 Program Contract Managers, the CDPH Privacy Officer, and the CDPH Chief 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 Contractor. Said changes shall not require an amendment to this Exhibit or the Agreement to which it is incorporated.

Exhibit D
HIPAA Business Associate Exhibit

CDPH Program Contract Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer Privacy Office, c/o Office of Legal Services California Department of Public Health P.O. Box 997377, MS 0505 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (916) 440-7671	Chief Information Security Officer Information Security Office California Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: IT Service 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 Exhibit 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 Exhibit, 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.

IV. Obligations of CDPH

CDPH agrees to:

A. ***Notice of Privacy Practices.*** Provide Business Associate with applicable and relevant Notice(s) of Privacy Practices that CDPH HIPAA-covered healthcare components produce in accordance with 45 CFR 164.520, as well as any changes to such notice(s).

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 D
HIPAA Business Associate Exhibit

V. 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 Exhibit. Business Associate shall promptly remedy any violation of any provision of this Exhibit and shall certify the same to the CDPH Privacy Officer or the CDPH Chief Information Security 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 Exhibit, nor does CDPH's:

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's enforcement rights under this Agreement and this Exhibit.

VI. Termination

A. ***Termination for Cause.*** Upon CDPH's knowledge of a material breach of this Exhibit 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 Exhibit 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 promptly 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 Exhibit 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.

VII. Miscellaneous Provisions

A. ***Disclaimer.*** CDPH makes no warranty or representation that compliance by Business Associate with this Exhibit, 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

Exhibit D
HIPAA Business Associate Exhibit

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 Exhibit 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's request, Business Associate agrees to promptly enter into negotiations with CDPH concerning an amendment to this Exhibit 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 Exhibit when requested by CDPH pursuant to this Section or

2) Business Associate does not enter into an amendment providing assurances regarding the safeguarding and security 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 Exhibit 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 Exhibit 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 Exhibit 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 Exhibit 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 VII.C of this Exhibit 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 D
HIPAA Business Associate Exhibit

Attachment 1
Business Associate Data Security Standards

1. General Security Controls

A. ***Confidentiality Statement.*** All persons that will be working with CDPH PHI must sign a confidentiality statement. The statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to CDPH PHI. The statement must be renewed annually. The Business Associate shall retain each person's written confidentiality statement for CDPH inspection for a period of three (3) years following contract termination.

B. ***Background check.*** Before a member of the Business Associate's workforce may access CDPH PHI, Business Associate 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. The Business Associate shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

C. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store CDPH PHI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the CDPH Information Security Office.

D. ***Server Security.*** Servers containing unencrypted CDPH PHI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

E. ***Minimum Necessary.*** Only the minimum necessary amount of CDPH PHI required to perform necessary business functions may be copied, downloaded, or exported.

F. ***Removable media devices.*** All electronic files that contain CDPH PHI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher

G. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store CDPH PHI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

H. ***Patch Management.*** All workstations, laptops and other systems that process and/or store CDPH PHI must have security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation

Exhibit D
HIPAA Business Associate Exhibit

timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

I. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing CDPH PHI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. 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 Sanitization.*** All CDPH PHI must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

2. System Security Controls

A. ***System Timeout.*** The system must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

B. ***Warning Banners.*** All systems containing CDPH 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 maintain an automated audit trail which can identify the user or system process which initiates a request for CDPH PHI, or which alters CDPH PHI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If CDPH PHI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

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 of CDPH PHI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing CDPH PHI can be encrypted. This requirement pertains to any type of CDPH PHI in motion such as website access, file transfer, and E-Mail.

Exhibit D
HIPAA Business Associate Exhibit

F. ***Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting CDPH PHI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

A. ***System Security Review.*** All systems processing and/or storing CDPH PHI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.

B. ***Log Reviews.*** All systems processing and/or storing CDPH PHI must have a routine procedure in place to review system logs for unauthorized access.

C. ***Change Control.*** All systems processing and/or storing CDPH 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. ***Disaster Recovery.*** Business Associate must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDPH PHI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.

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

5. Paper Document Controls

A. ***Supervision of Data.*** CDPH 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. CDPH 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. ***Escorting Visitors.*** Visitors to areas where CDPH PHI is contained shall be escorted and CDPH Protected Health Information shall be kept out of sight while visitors are in the area.

C. ***Confidential Destruction.*** CDPH PHI must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

Exhibit D
HIPAA Business Associate Exhibit

D. ***Removal of Data.*** CDPH PHI must not be removed from the premises of the Business Associate except with express written permission of CDPH.

E. ***Faxing.*** Faxes containing CDPH 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 with the intended recipient before sending.

F. ***Mailing.*** CDPH PHI shall only be mailed using secure methods. Large volume mailings of CDPH Protected Health Information 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 CDPH approved solution, such as a solution using a vendor product specified on the CSSI.

CCC-307

CERTIFICATION

I, the official named below, CERTIFY UNDER PENALTY OF PERJURY that I am duly authorized to legally bind the prospective Contractor to the clause(s) listed below. This certification is made under the laws of the State of California.

Contractor/Bidder Firm Name (Printed)	*Federal ID Number*
By (Authorized Signature)	
Printed Name and Title of Person Signing	
Date Executed	*Executed in the County of*

CONTRACTOR CERTIFICATION CLAUSES

1. STATEMENT OF COMPLIANCE: Contractor has, unless exempted, complied with the nondiscrimination program requirements. (Gov. Code §12990 (a-f) and CCR, Title 2, Section 8103) (Not applicable to public entities.)

2. DRUG-FREE WORKPLACE REQUIREMENTS: Contractor will comply with the requirements of the Drug-Free Workplace Act of 1990 and will provide a drug-free workplace by taking the following actions:

a. Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations.

b. Establish a Drug-Free Awareness Program to inform employees about:

1) the dangers of drug abuse in the workplace;
2) the person's or organization's policy of maintaining a drug-free workplace;
3) any available counseling, rehabilitation and employee assistance programs; and,
4) penalties that may be imposed upon employees for drug abuse violations.

c. Every employee who works on the proposed Agreement will:

1) receive a copy of the company's drug-free workplace policy statement; and,
2) agree to abide by the terms of the company's statement as a condition of employment on the Agreement.

Failure to comply with these requirements may result in suspension of payments under the Agreement or termination of the Agreement or both and Contractor may be ineligible for award of any future State agreements if the department determines that any of the following has occurred: the Contractor has made false certification, or violated the

or the Department of Justice to determine the contractor's compliance with the requirements under paragraph (a).

7. DOMESTIC PARTNERS: For contracts over $100,000 executed or amended after January 1, 2007, the contractor certifies that contractor is in compliance with Public Contract Code section 10295.3.

DOING BUSINESS WITH THE STATE OF CALIFORNIA

The following laws apply to persons or entities doing business with the State of California.

1. CONFLICT OF INTEREST: Contractor needs to be aware of the following provisions regarding current or former state employees. If Contractor has any questions on the status of any person rendering services or involved with the Agreement, the awarding agency must be contacted immediately for clarification.

Current State Employees (Pub. Contract Code §10410):

1). No officer or employee shall engage in any employment, activity or enterprise from which the officer or employee receives compensation or has a financial interest and which is sponsored or funded by any state agency, unless the employment, activity or enterprise is required as a condition of regular state employment.

2). No officer or employee shall contract on his or her own behalf as an independent contractor with any state agency to provide goods or services.

Former State Employees (Pub. Contract Code §10411):

1). For the two-year period from the date he or she left state employment, no former state officer or employee may enter into a contract in which he or she engaged in any of the negotiations, transactions, planning, arrangements or any part of the decision-making process relevant to the contract while employed in any capacity by any state agency.

2). For the twelve-month period from the date he or she left state employment, no former state officer or employee may enter into a contract with any state agency if he or she was employed by that state agency in a policy-making position in the same general subject area as the proposed contract within the 12-month period prior to his or her leaving state service.

If Contractor violates any provisions of above paragraphs, such action by Contractor shall render this Agreement void. (Pub. Contract Code §10420)

Members of boards and commissions are exempt from this section if they do not receive payment other than payment of each meeting of the board or commission, payment for preparatory time and payment for per diem. (Pub. Contract Code §10430 (e))

Darfur Contracting Act

Pursuant to Public Contract Code (PCC) sections 10475-10481, the Darfur Contracting Act's intent is to preclude State agencies from contracting with scrutinized companies that do business in the African nation of Sudan. A scrutinized company is a company doing specified types of business in Sudan as defined in PCC section 10476. Scrutinized companies are ineligible to, and cannot, contract with a State agency for goods or services (PCC section 10477(a)) unless obtaining permission from the Department of General Services according to the criteria set forth in PCC section 10477(b).

Therefore, to be eligible to contract with the California Department of Public Health, please initial **one of the following** three paragraphs and complete the certification below:

1. _____ Initials — We do not currently have, or we have not had within the previous three years, business activities or other operations outside of the United States.

OR

2. _____ Initials — We are a scrutinized company as defined in Public Contract Code section 10476, but we have received written permission from the Department of General Services (DGS) to submit a bid or proposal pursuant to Public Contract Code section 10477(b) or submit a contract/purchase order. A copy of the written permission from DGS is included with our bid, proposal or contract/purchase order.

OR

3. _____ Initials — We currently have, or we have had within the previous three years, business activities or other operations outside of the United States, but we certify below that we are not a scrutinized company as defined in Public Contract Code section 10476.

CERTIFICATION

I, the official named below, CERTIFY UNDER PENALTY OF PERJURY that I am duly authorized to legally bind this company to the clause listed above. This certification is made under the laws of the State of California.

Company Name (Printed)	*Federal ID Number*
By (Authorized Signature)	
Printed Name and Title of Person Signing	
Date Executed	*Executed in the County and State of*