

**34415**


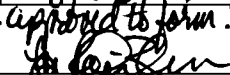

REGISTRATION NUMBER	AGREEMENT NUMBER 16-10341
---------------------	------------------------------

- 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)  
**City of Long Beach**
- The term of this Agreement is: **July 1, 2016 through June 30, 2019**
- The maximum amount of this Agreement is: **\$ 0**  
 Zero dollar contract solely based on usage
- 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	14 pages
Exhibit AI – Definition of Terms	2 pages
Exhibit B – Budget Detail and Payment Provisions	3 pages
Exhibit C * – General Terms and Conditions	<u>GTC 610</u>
Exhibit D – HIPAA Business Associate Addendum	15 pages
Exhibit E – Notice of Privacy Practices	4 pages
Exhibit F – Security Requirements, Protections, and Confidentiality Checklist	1 page
Exhibit G – Plan for Transporting Confidential ADAP Client Files (Policy and Procedure)	2 pages
Exhibit H – Non Discrimination Clause	1 page
Exhibit I – Confidentiality Requirements	1 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		<b>California Department of            General Services Use Only</b>
CONTRACTOR'S NAME (if other than an individual, state whether a corporation, partnership, etc.) <b>City of Long Beach Assistant City Manager</b>		
BY (Authorized Signature) 	EXECUTED PURSUANT TO SECTION 301 OF THE CITY CHARTER. <b>8/25/16</b> <i>Approved to form:</i>  <b>Long Beach Dep. C.A.</b> <b>8/28/16</b>	
PRINTED NAME AND TITLE OF PERSON SIGNING <b>Patrick H. West, City Manager</b>		
ADDRESS <b>2525 Grand Avenue            Long Beach, CA 90815</b>		
STATE OF CALIFORNIA		
AGENCY NAME <b>California Department of Public Health</b>		
BY (Authorized Signature) 	DATE SIGNED (Do not type) <b>9/19/16</b>	
PRINTED NAME AND TITLE OF PERSON SIGNING <b>for Yolanda Murillo, Chief, Contracts Management Unit</b>		
ADDRESS <b>1616 Capitol Avenue, Suite 74.317, MS 1802, PO Box 997377            Sacramento, CA 95899-7377</b>		

Exempt per: OA Budget Act 2016

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

**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 Human Immunodeficiency Virus (HIV) and Acquired Immunodeficiency Syndrome (AIDS).

The Contractor agrees to provide CDPH/OA, the services described herein for the provision of the AIDS Drug Assistance Program (ADAP) enrollment services, which includes both ADAP's Medication Program and Health Insurance Assistance Programs. This contract agreement will be in effect for three consecutive fiscal years (FY) beginning in FY 2016-17 through FY 2018-19 (July 1, 2016 – June 30, 2019).

Refer to Exhibit A, Attachment I, "Definitions of Terms" to review definitions of acronyms and other contract related terms and references.

**2) Service Location**

The services shall be performed at the City of Long Beach Department of Health and Human Services, located at 2525 Grand Avenue, Long Beach, CA 90815.

**3) Service Hours**

The services shall be provided during normal Contractor working hours.

**4) Project Representatives**

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

<b>California Department of Public Health</b> OA ADAP Branch Chief Niki Dhillon  Telephone: (916) 449-5942 Fax: (916) 449-5859 Email: Niki.Dhillon@cdph.ca.gov	<b>City of Long Beach</b> City Manager Patrick H. West  Telephone: (562) 570-4341 Fax: (562) 570-4374 Email: sarady.kong@longbeach.gov
--	--

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

B. Direct all inquiries to:

<b>California Department of Public Health</b> OA ADAP Advisor Kathy Nguyen  MS 7700, P.O. Box 997426 1616 Capitol Avenue, Suite 616 Sacramento, CA 95899-7426  Telephone: (916) 449-5924 Fax: (916) 449-4909 Email: <a href="mailto:kathy.nguyen@cdph.ca.gov">kathy.nguyen@cdph.ca.gov</a>	<b>City of Long Beach</b> ADAP Enrollment Worker Rosie Gutierrez-Tufuga  2525 Grand Avenue Long Beach, CA 90815  Telephone: (562) 570-4316 Fax: Email: <a href="mailto:rosie.gutierrez-tufuga@longbeach.gov">rosie.gutierrez-tufuga@longbeach.gov</a>
--	--

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.

**Exhibit A**

Scope of Work

July 1, 2016 through June 30, 2019

- 5) **Services to be Performed**
  - A) **Major Function, Task and Activities**

The Contractor shall:

Enrollment Site Requirements:	Time Line	Responsible Party	Performance Measure and/or Deliverables
<p><b>A.1. ADAP Enrollment Site Contact Requirement:</b></p> <p>Maintain an ADAP Enrollment Site Contact to ensure compliance with the requirements of this contract agreement on behalf of the ADAP Enrollment Site and facilitate required information exchange between the Enrollment Site, CDPH/OA/ADAP, and CDPH/OA/ADAP's contracted EBM.</p>	<p>Throughout the life of the contract</p>	<p>Authorized Site Administrator</p>	<p>ADAP Site Contact Name and contact information must be identified in Section 4B. Provide written notice to the assigned ADAP Advisor immediately of any changes to the ADAP Enrollment Site Contact.</p>
<p><b>A.2. Nondiscrimination Requirements:</b></p> <p>Comply with the provisions as stated in Exhibit H, "Nondiscrimination Clause" (STD 17A)." The ADAP Enrollment Site shall not unlawfully discriminate against any employee or applicant for employment because of race, religion, color, national origin, ancestry, physical handicap, medical condition, marital status, age, sex, or sexual orientation.</p>	<p>Must be maintained through the life of the contract</p>	<p>Authorized Site Administrator /Agency's EEO Officer</p>	<p>Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", Exhibit F.</p>

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

<p><b>A.3. Information Privacy and Security Requirements:</b></p> <p>All personnel conducting ADAP enrollment services must abide by all applicable laws and CDPH/OA/ADAP guidelines regarding confidentiality of ADAP client eligibility files and protected health information when accessing or submitting ADAP client data.</p>			
<p>i. Ensure compliance with the provisions as stated in Exhibit D, "HIPAA Business Associate Addendum (CDPH HIPAA BAA 8-14).</p>	<p>Must be maintained through the life of the contract. Contractor shall also continue to extend the protections of these provisions to protected health information upon termination or expiration of the agreement until its return or destruction.</p>	<p>ADAP Enrollment Site Contact</p>	<p>Notify the assigned ADAP Advisor immediately by phone call plus email or fax when a potential breach has occurred. ADAP EWs may be deactivated if more than two potential breaches occur within a calendar year. Enrollment Sites may also be deactivated if potential breaches are committed by more than two EWs in a calendar year.</p>
<p>ii. Ensure that all ADAP EWs employed by or volunteering at the Enrollment Site are issued/assigned an Agency email address.</p>	<p>At the time of ADAP EW activation and throughout the</p>	<p>Authorized Site Administrator /Site Contact</p>	<p>Verified when ADAP Enrollment Worker(s) email address is provided to assign CDPH/OA/ADAP Advisor.</p>

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

ADAP EWs are prohibited from using a personal email address (i.e. gmail, yahoo, etc.) for ADAP related correspondence.	life of the contract.		
<p>iii. Ensure compliance with the provisions as stated in "Exhibit E, "Notice of Privacy Practices", and ensure that the notice is posted at the Enrollment Site.</p>	<p>Must be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact</p>	<p>Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", Exhibit F.</p>
<p>iv. Review and sign the "Agreement by Employee/Contractor to Comply with Confidentiality Requirements (CDPH 8689)" form (Exhibit I).</p>	<p>Annually</p>	<p>ADAP Enrollment Site Contact and ADAP EW(s)</p>	<p>Submit completed CDPH 8689 form via the EBM upon completion of new or existing ADAP EW training. Site Contacts who are not EWs must submit the 8689 to their assigned ADAP Advisor.</p>
<p>v. Ensure that only certified ADAP EWs have access to ADAP client eligibility file information, unless otherwise authorized by law. Please refer to the following confidentiality table and flowchart that pertains to your ADAP enrollment site:</p> <ul style="list-style-type: none"> <li>• For a Community Based Organization go to: <a href="http://www.cdph.ca.gov/programs/aids/Documents/ADAPSite-CBO-TableFlowchart.pdf">http://www.cdph.ca.gov/programs/aids/Documents/ADAPSite-CBO-TableFlowchart.pdf</a></li> <li>• For a Health Care Provider – go to: <a href="http://www.cdph.ca.gov/programs/aids/Documents/ADAPSite-HCP-TableFlowchart.pdf">http://www.cdph.ca.gov/programs/aids/Documents/ADAPSite-HCP-TableFlowchart.pdf</a></li> <li>• For a Local Public Health Department – go to: <a href="http://www.cdph.ca.gov/programs/aids/Documents/ADAPSite-PHD-TableFlowchart.pdf">http://www.cdph.ca.gov/programs/aids/Documents/ADAPSite-PHD-TableFlowchart.pdf</a></li> </ul>	<p>Must be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact and ADAP EW(s)</p>	<p>Notify the assigned ADAP Advisor immediately when a potential breach has occurred.</p>

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

<p><b>A.4. ADAP Enrollment Site Information Technology/Equipment Requirements:</b></p>	<p>By the go-live date and to be maintained through the life of the contract.</p>	<p>Authorized Site Administrator and ADAP Enrollment Site Contact</p>	<p>All client enrollments must occur electronically via the EBM secure web-based enrollment system.</p>
<p>i. Ensure internet access and equipment to scan and upload ADAP applicant/client eligibility documents to the CDPH/OA/ADAP's EBM secure web-based enrollment system.</p>	<p>By the go-live date and to be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact</p>	<p>Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", Exhibit F.</p>
<p>ii. Only desktop computers are to be used to conduct ADAP enrollment services. The use of laptop computers or other hand held electronic devices are strictly prohibited for use in ADAP client enrollment.</p>	<p>By the go-live date and to be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact</p>	<p>Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", Exhibit F.</p>
<p>iii. Ensure that fax machines and CDPH/OA/ADAP fax/scanners used to upload and submit ADAP applications or receive ADAP correspondence, which may include confidential client information, are located in a secure area.</p>	<p>By the go-live date and to be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact</p>	<p>Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", Exhibit F.</p>

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2019

<p><b>A.5. Quality Requirements</b></p> <p>ADAP EWs and Enrollment Sites will be held to quality standards. EWs are required to maintain an ADAP enrollment performance level of at least 95 percent accuracy for ADAP eligibility documentation and enrollment. Enrollment Sites are required to maintain a minimum performance level of 90 percent. CDPH/OA/ADAP will conduct secondary review on all ADAP applications. Applications with errors will be considered defective and will count against the performance level of the ADAP EW/Enrollment Site. ADAP EW/Enrollment Site quality will be factored by dividing the number of defective applications by the total number of applications processed.</p>	<p>To be maintained through the life of the contract</p>	<p>ADAP Enrollment Site Contact and ADAP EW(s)</p>	<p>i. CDPH/OA/ADAP will monitor performance levels for the first year and provide performance reports and technical assistance.</p> <p>ii. If after the first quarter following the initial one year monitoring period, an ADAP EW(s)/Enrollment Site has an error rate that exceeds the quality standard, the Site Contact must submit a Corrective Action Plan to the ADAP Advisor for approval.</p> <p>ii. If an ADAP EW(s)/ Enrollment Site remains deficient for a second consecutive quarter, CDPH/OA/ADAP may suspend the Enrollment Worker for defective ADAP applications processed during the quarter.</p>
--	--	--	--



**Exhibit A**

Scope of Work

July 1, 2016 through June 30, 2019

<p><b>A.6. Conduct Requirements:</b></p> <p>ADAP EWs are required to conduct themselves with a high degree of professionalism and integrity. Site Contacts are required to ensure that no ADAP EW is employed by nor receives any financial compensation (including gifts or any other type of incentive) from a participating ADAP pharmacy and that no ADAP client enrollment is conducted at any participating ADAP pharmacy location.</p> <p>Additional examples of misconduct include, but are not limited to:</p>	<p>To be maintained through the life of the contract</p>	<p>ADAP Enrollment Site Contact and ADAP EW(s)</p>	<p>v. If an ADAP EW(s)/Enrollment Site remains deficient for a third consecutive quarter, the EW(s)/Enrollment Site may be deactivated and will no longer be allowed to perform ADAP enrollment.</p>
		<p>Notify the ADAP Advisor when instances of misconduct are identified.</p> <p>ADAP Site Contacts may be required to submit a Corrective Action Plan to the ADAP Advisor to address occurrences of misconduct.</p>	

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2019

<p>i. Knowingly and willfully enrolling clients with inaccurate or false documentation.*          ii. Insubordination and/or non-compliance with CDPH/OA/ADAP staff requests.          iii. Verbally abusive, use of derogatory language          iv. Unresponsive to CDPH/OA/ADAP staff and/or client inquiries.          v. Conducting unauthorized off-site ADAP enrollment.          vi. Transporting ADAP files without having a transportation plan approved by CDPH/OA/ADAP staff.</p> <p>* Knowingly providing inaccurate or false documentation may be in violation of various Penal Code laws and may be subject to violations of the California False Claims Act, which prohibits any person or entity from knowingly making or using a false statement or document to obtain money, property, or services from the State. (See California Government Code section 12650 et. seq.)</p>		<p>EWs who engage in misconduct may be subject to temporary or permanent suspension of ADAP EW status.</p>
<p><b>A.7. Training and Guidelines Requirements:</b></p> <p>i. Ensure all new ADAP EWs have successfully completed new ADAP EW training provided by CDPH/OA/ADAP prior to enrolling or re-certifying ADAP clients.</p>	<p>To be maintained through the life of the contract.</p>	<p>Report to the assigned ADAP Advisor, site staff who will be registering for required ADAP EW trainings.</p>

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

<p>ii. Ensure compliance with the requirements written in the ADAP "California State ADAP Guidelines" and ADAP Management Memos.</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact and ADAP EW(s)</p>	<p>Notify ADAP EWs to recertify 30 days prior to the recertification end date.</p>
<p>iii. Ensure existing ADAP EWs maintain active status by participating in required annual recertifying ADAP EW trainings and/or other required ad hoc trainings provided by CDPH/OA/ADAP and/or the CDPH/OA/ADAP EBM in order to maintain ADAP certification to continue conducting ADAP enrollment functions.</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact</p>	<p>Must ensure ADAP Enrollment Site participation for 90 percent of these calls. Must contact the ADAP Advisor, if unable to participate on a call to discuss the topics covered.</p>
<p>iv. Ensure the ADAP Enrollment Site has representation/participation on all monthly CDPH/OA/ADAP EW calls.</p>	<p>Monthly through the life of the contract.</p>	<p>ADAP Enrollment Site Contact</p>	<p>This site specific ADAP EW ID number may only be used by the ADAP EW to whom it is assigned for enrollment activities at this site.</p>
<p><b>A.8.ADAP Enrollment Tracking Requirements:</b></p>		<p>i. Ensure all ADAP EWs are identified and have a site specific ADAP EW ID number issued by the CDPH/OA/ADAP EBM.</p>	<p>ADAP Enrollment Site Contact</p>

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

<p>ii. Report any changes in site specific ADAP EWs' status (e.g., job duties, relocation, separation, etc.) that will alter the ADAP EW(s) ability to enroll clients, including the de-activation of any ADAP EW ID numbers.</p>	<p>Within 24 hours of the change</p>	<p>ADAP Enrollment Site Contact</p>	<p>Report addition/deletion/changes to ADAP EW(s) to the CDPH/OA/ADAP EBM and/or the assigned ADAP Advisor.</p>
<p><b>A.9. Transportation Plan Requirements:</b> Ensure that no ADAP client eligibility documentation, records, files, etc., will be transported to or from the ADAP Enrollment Site without an approved transportation plan.</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact</p>	<p>See "Plan for Transporting Confidential ADAP Client Files", Exhibit G.</p>
<p>Exception to this restriction may be approved by CDPH/OA/ADAP for the following reasons:</p> <ul style="list-style-type: none"> <li>i. Client disability; or,</li> <li>ii. Remote distance requires ADAP EW to meet with client outside of the ADAP Enrollment Site; or,</li> <li>iii. The entire ADAP Enrollment Site is moving to a new address/location.</li> </ul> <p>Ensure that no ADAP client enrollment files will be transported until CDPH/OA/ADAP provides written approval of the site's specific transportation plan.</p>	<p>30 days prior to the need for transporting any ADAP client enrollment documents/files</p>	<p>ADAP Enrollment Site Contact</p>	<p>Submit a written request to the assigned ADAP Advisor which justifies the necessity for transporting ADAP client enrollment document/files. The request must also identify the specific procedures to be followed to safeguard the confidentiality of the ADAP client documents being transported, as well as who will be responsible/accountable for site's specific procedure(s). See "Plan for Transporting Confidential ADAP Client Files", Exhibit G.</p>
<p><b>A.10. Administrative Requirements</b></p> <ul style="list-style-type: none"> <li>i. Notify the assigned ADAP Advisor if the site wishes to change from an open site (one which serves any individual who wishes to enroll) to a closed site (one</li> </ul>	<p>Within at least 30 days notice to the requested change in status date.</p>	<p>ADAP Enrollment Site Contact</p>	<p>Written Request required (may be submitted by email) to ADAP Advisor.</p>

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

<p>which serves only agency-affiliated individuals) or vice versa.</p>			
<p>ii. Notify the assigned ADAP Advisor if the site plans to no longer provide ADAP enrollment services.</p>	<p>ADAP Enrollment Site Contact/Authorized Agency Administrator</p>	<p>Written Notification required (may be submitted by email) and submission of an ADAP transportation plan to the site's designated ADAP Advisor assuring the secure transfer of hard copy ADAP client files.</p>	
<p><b>A.11. Auditing Requirements</b></p>			
<p>A. Facilitate CDPH/OA/ADAP site visit requests, including but not limited to receiving or providing required documentation/information as requested by the assigned ADAP Advisor. Act as liaison between the site, ADAP Advisor, ADAP EW(s), and LHJ Coordinator (if applicable) in activities related to the site visit.</p>	<p>As needed during normal working hours</p>	<p>ADAP Site Contact/Authorized Agency Administrator</p>	<p>Respond to written notifications and requests for information initiated by CDPH/OA/ADAP personnel.</p>
<p>B. Ensure that CDPH/OA/ADAP staff, authorized CDPH/OA/ADAP representatives and/or other state and federal agencies are granted access to all ADAP client eligibility files and any other documentation related to this contract agreement for audit purposes.</p>	<p>As needed during normal working hours</p>	<p>ADAP Site Contact/Authorized Agency Administrator</p>	<p>Respond to written and in-person requests for ADAP client files made by CDPH/OA/ADAP personnel.</p>

**Exhibit A**  
Scope of Work  
July 1, 2016 through June 30, 2019

<p>C. Develop and submit required Corrective Action Plan (CAP) when required based on results of ADAP site visit/federal or state program audit.</p>	<p>As needed</p>	<p>ADAP Site Contact/Authorized Agency Administrator</p>	<p>CAP is to be submitted to the assigned ADAP Advisor by the timeframe identified in the letter or audit report indicating the CAP is required.</p>
<p>D. Maintain hard copy ADAP client files/records for four years (the current year, plus three prior years).</p>	<p>To be maintained through the life of the contract.</p>	<p>ADAP Enrollment Site Contact</p>	<p>As needed, records will be made available to view within the timeframe provided by the federal or state auditors.</p> <p>At contract termination or expiration, Protected Health Information must be returned or retained in accordance with Exhibit D, "HIPAA Business Associate Addendum (CDPH HIPAA BAA 8-14)".</p>
<p><b>A.12. Grievance Requirements</b></p> <p>A. Ensure that ADAP clients are made aware of, and have access to, the CDPH/OA/ADAP Grievance procedures, and form as outlined in the California State ADAP Guidelines.</p>	<p><b>During in-person services</b></p> <p>Upon initial and annual re-enrollments of ADAP clients.</p>	<p>ADAP Enrollment Site Contact and/or ADAP EW(s)</p>	<p>CDPH/OA/ADAP will verify, via review of the ADAP Client Satisfaction Survey.</p>

**Exhibit A**  
 Scope of Work  
 July 1, 2016 through June 30, 2019

<p>B. Upon client request, assist ADAP clients in the completion and submission of a CDPH/OA/ADAP grievance form and related documents. Assistance may also include providing the mailing address and contact information for ADAP Advisors and/or other CDPH/OA/ADAP Contractors, and/or the submission of the completed grievance form and related documents to CDHP/OA/ADAP.</p>	<p>As needed</p>	<p>ADAP        Enrollment        Site Contact        and/or ADAP        EW(s)</p>	<p>Notify the assigned ADAP Advisor immediately if assistance is needed with the CDPH/OA/ADAP grievance process.</p>
---	------------------	---	--

**Exhibit A, Attachment I**  
Definition of Terms

- i. AIDS Drug Assistance Program (ADAP) – Established in 1987 to help ensure that eligible, HIV positive uninsured and under-insured individuals have access to medication on the ADAP formulary through the Medication Program and Health Insurance Assistance Programs. ADAP provides medication, premium payment, and medical out of pocket payment assistance.
- ii. ADAP Advisor – Office of AIDS ADAP staff assigned to a Local Health Jurisdiction or ADAP Enrollment Site for monitoring and technical assistance.
- iii. ADAP Coordinator – Local Health Jurisdiction or other local agency staff designated to act as the primary county contact between the ADAP enrollment sites, OA, and ADAP contractors.
- iv. ADAP Enrollment Worker (EW) – ADAP Enrollment Site staff certified to provide ADAP enrollment services and access ADAP data.
- v. ADAP Enrollment Site Contact – Ensures the requirements of this contract agreement are adhered to, including, but not limited to the participation in monthly ADAP EW calls. Act as the primary contact for OA, the ADAP Coordinator within the Local Health Jurisdiction, and ADAP service contractors.
- vi. California Department of Public Health (CDPH) – is the lead agency in California providing detection, treatment, prevention and surveillance of public health issues.
- vii. Closed Site – ADAP enrollment site that only serves ADAP applicants/clients associated with their entity.
- viii. Community Based Organization (CBO) – Non-profit 501(3)(c) entities that operate within a single local community.
- ix. Fiscal Year (FY) – July 1 through June 30.
- x. Contractor – ADAP approved enrollment site managed by a non-profit organization to provide ADAP enrollment services.
- xi. Enrollment Benefits Manager (EBM) – Service contractor providing enrollment and benefits management support for ADAP.
- xii. Insurance Benefits Manager (IBM) – Service contractor that manages and processes health insurance premium payments for clients enrolled in both ADAP's Medication Program and Insurance Assistance Programs.
- xiii. Local Health Jurisdiction (LHJ) – One of 58 counties and three cities (Pasadena, Long Beach, and Berkeley) in the state of California.
- xiv. Medical Benefits Manager (MBM) – Service contractor that manages and processes outpatient medical out of pocket payments for clients enrolled in both ADAP's Medication Program the Office of AIDS Health Insurance Premium Payment Program.



**Exhibit A, Attachment I**  
Definition of Terms

- xv. Office of AIDS (OA) – Has lead responsibility for coordinating state programs, services, and activities relating to HIV/AIDS as designated by California Health and Safety Code Section 131019.
- xvi. OA Health Insurance Premium Payment (OA-HIPP) – Pays for private health insurance premiums and medical out of pocket costs for clients co-enrolled in ADAP's Medication Program.
- xvii. OA Medicare Part D Premium Payment Program – Pays for Medicare Part D premiums for clients co-enrolled in ADAP's Medication Program.
- xviii. Open Site – ADAP enrollment site that serves all ADAP applicants/clients.
- xix. Pharmacy Benefits Manager (PBM) – Service contractor administering the ADAP statewide pharmacy network and providing pharmaceutical services for ADAP clients

**Exhibit B**  
Budget Detail and Payment Provisions

**1. Payments**

- A. In no event shall CDPH/OA/ADAP pay the Contractor for services performed prior to the commencement date or after the expiration of this Agreement.
- B. For services satisfactorily rendered, CDPH/OA/ADAP agrees to compensate the Contractor for actual services provided in accordance with the amounts specified in Exhibit B, Section E., Amounts Payable.
- C. Payments shall be processed by CDPH/OA/ADAP no later than the end of the quarter dates noted below.

First Quarter:                      July 1 – September 30  
Payment no later than:              November 30

Second Quarter:                      October 1 – December 31  
Payment no later than:              February 28

Third Quarter:                      January 1 – March 31  
Payment no later than:              May 31

Fourth Quarter:                      April 1 – June 30  
Payment no later than:              August 31

(FINAL) Supplemental:              July 1 – June 30  
Payment no later than:              August 31

D. Payments shall:

- 1) Be calculated based on current ADAP client enrollment data as provided by the ADAP Enrollment Benefits Management (EBM) contractor to determine the number of ADAP services provided at each enrollment site.
- 2) Identify the payment period and/or performance period covered.
- 3) Itemize ADAP services for the payment period in the same level of detail as indicated in Section E Amounts Payable. Subject to the terms of this agreement, payment will only be made for those services expressly identified in this agreement as approved by CDPH/OA/ADAP.

**E. Amounts Payable**

All ADAP enrollment sites with a minimum of one ADAP enrollment per fiscal year (FY) will receive a floor amount of \$5,000 with additional payment(s) per FY for performing the following ADAP services complete with all required forms and verifying documentation:

- New ADAP Medication Program Enrollments: \$50/per new enrollment

**Exhibit B**  
Budget Detail and Payment Provisions

- New ADAP Insurance Assistance Program Enrollments: \$100/per new enrollment
- ADAP bi-annual recertifications: \$20/per recertification
- ADAP annual re-enrollments: \$50/per re-enrollment
- Covered California open enrollment annual renewal documentation submissions for OA-HIPP/Covered California clients (may be required outside clients' enrollment or recertification cycle for new health plan year): \$50/per renewal
- ADAP Client Updates: \$20/per update related to income, residency, and health insurance/other third party payer coverage.

**2. Budget Contingency Clause**

- A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to the Contractor, or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.
- B. If funding for any FY is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Agreement with no liability occurring to the State, or offer an agreement amendment to the Contractor to reflect the reduced amount.
- C. In the event of early termination or cancellation, the Contractor shall be entitled to compensation for services performed satisfactorily under this agreement and expenses incurred up to the date of termination or cancellation and any non-cancelable obligations incurred in support of this agreement.

**3. Prompt Payment Clause**

Payment will be made in accordance with, and within the time specified in, Government Code Chapter 4.5, commencing with Section 927.

**4. Timely Final Payment**

- A. Final payment shall be processed no more than *sixty (60)* calendar days following the expiration or termination date of this agreement, unless a later or alternate deadline is agreed to in writing by the program contract manager.
- B. CDPH/OA/ADAP shall make payment to the Contractor quarterly in arrears for costs associated with the provision of ADAP services at the ADAP Enrollment Site in the local health jurisdiction (LHJ), under this contract agreement. Payment to the Contractor will be contingent upon receipt and execution of this contract agreement and the provision of ADAP services (as verified by CDPH/OA/ADAP through the EBM data).
- C. This contract agreement is subject to any additional restrictions, limitations, or conditions enacted by the Congress or the State Legislature, which may affect the provisions, terms, or funding of this contract agreement in any manner.

**Exhibit B**  
Budget Detail and Payment Provisions

**5. Recovery of Overpayments**

- A. Contractor agrees that payments based upon the terms of this agreement or an audit finding and/or an audit finding that is appealed and upheld, will be recovered by CDPH/OA/ADAP by CDPH/OA/ADAP withholding payments or withholding a portion of payment for services performed until the amount of overpayment has been resolved.

If the Contractor has filed a valid appeal regarding the report of audit findings, recovery of the overpayments will be deferred until a final administrative decision on the appeal has been reached.

Exhibit D  
HIPAA Business Associate Addendum

**I. Recitals**

- A. The underlying contract (Agreement), to which this HIPAA Business Associate Addendum is attached to and made a part of, has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the HITECH Act"), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").
- B. The Department of Public Health ("CDPH") wishes to disclose to Business Associate certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.
- C. As set forth in the Agreement, Contractor, here and after, is the Business Associate of CDPH acting on CDPH' behalf and 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 and PI. CDPH and Business Associate are each a party to the Agreement and are collectively referred to as the "parties."
- D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to the Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that CDPH must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act.
- E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

**II. Definitions**

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.
- E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.

Exhibit D  
HIPAA Business Associate Addendum

- F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.
- G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164.
- H. Personal Information shall have the meaning given to such term in California Civil Code section 1798.29.
- I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.
- J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, 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.
- M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act and the HIPAA regulations.

### III. Terms of Agreement

#### A. Permitted Uses and Disclosures of PHI by Business Associate

**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 the Agreement, for, or on behalf of CDPH, provided that such use or disclosure would not violate the HIPAA regulations, if done by CDPH. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the

Exhibit D  
HIPAA Business Associate Addendum

minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

1. **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Addendum, Business Associate may:
  - a. **Use and disclose for management and administration.** Use and disclose PHI for the proper management and administration of the Business Associate provided that such 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.
  - b. **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.

**B. Prohibited Uses and Disclosures**

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).
2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CDPH and as permitted by 42 U.S.C. section 17935(d)(2).

**C. Responsibilities of Business Associate**

Business Associate agrees:

1. **Nondisclosure.** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by the Agreement or as required by law.
2. **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, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by the Agreement. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. 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 3, Security, below. Business Associate will provide CDPH with its current and updated policies.

Exhibit D  
HIPAA Business Associate Addendum

3. **Security.** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
  - a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;
  - b. 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 the Agreement;
  - c. 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
  - d. 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 the 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 and Subcontractors.**

1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of CDPH, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI and PI. Business Associate shall incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PI be reported to Business Associate.
2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:
  - a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by CDPH; or



Exhibit D  
HIPAA Business Associate Addendum

- b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

**F. Availability of Information to CDPH and Individuals.** To provide access and information:

1. 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.
2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable CDPH to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).
3. If Business Associate receives data from CDPH that was provided to CDPH by the Social Security Administration, upon request by CDPH, Business Associate shall provide CDPH with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

**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' compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to CDPH and shall set forth the efforts it made to obtain the information.

**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 the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for CDPH as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for CDPH after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is

Exhibit D  
HIPAA Business Associate Addendum

later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

**J. Breaches and Security Incidents.** During the term of the Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

1. **Notice to CDPH.** (1) To notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to CDPH by the Social Security Administration. (2) To notify CDPH **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of the Agreement and this Addendum, or potential loss of confidential data affecting the Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

Notice shall be provided to the CDPH Program 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, notice shall be provided by calling the CDPH ITSD Service Desk. Notice shall be made using the "CDPH Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the CDPH Privacy Office website ([www.CDPH.ca.gov](http://www.CDPH.ca.gov)),

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

- a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
2. **Investigation and Investigation Report.** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. Within 72 hours of the discovery, Business Associate shall submit an updated "CDPH Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer:
  3. **Complete Report.** To provide a complete report of the investigation to the CDPH Program Contract Manager, 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 be submitted on the "CDPH Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If CDPH requests information in addition to that listed on the "CDPH Privacy Incident Report" form, Business Associate shall make reasonable efforts to

Exhibit D  
 HIPAA Business Associate Addendum

provide CDPH with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "CDPH Privacy Incident Report" form. CDPH will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.

4. **Notification of Individuals.** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.
  
5. **Responsibility for Reporting of Breaches.** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach immediately upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to CDPH in addition to Business Associate, Business Associate shall notify CDPH, and CDPH and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.
  
6. **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 Addendum or the Agreement to which it is incorporated.

CDPH Program Contract Manager	CDPH Privacy Officer	CDPH 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 0506 Sacramento, CA 95899-7377  Email: <a href="mailto:privacy@cdph.ca.gov">privacy@cdph.ca.gov</a> Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413  Email: <a href="mailto:cdphiso@cdph.ca.gov">cdphiso@cdph.ca.gov</a> Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

Exhibit D  
HIPAA Business Associate Addendum

- K. Termination of Agreement.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by CDPH of this Addendum, it shall take the following steps:
1. Provide an opportunity for CDPH to cure the breach or end the violation and terminate the Agreement if CDPH does not cure the breach or end the violation within the time specified by Business Associate; or
  2. Immediately terminate the Agreement if CDPH has breached a material term of the Addendum and cure is not possible.
- L. Due Diligence.** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.
- M. Sanctions and/or Penalties.** Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

#### IV. 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 section 164.520, as well as any changes to such notice.
- 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 section 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.

#### V. Audits, Inspection and Enforcement

- A.** From time to time, CDPH may inspect the facilities, systems, books and records of Business Associate to monitor compliance with the 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:

Exhibit D  
HIPAA Business Associate Addendum

1. Failure to detect or
  2. 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 the Agreement and this Addendum.
- B. If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify CDPH and provide CDPH with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

## VI. Termination

- A. **Term.** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the Agreement and shall terminate when all the PHI provided by CDPH to Business Associate, or created or received by Business Associate on behalf of CDPH, is destroyed or returned to CDPH, in accordance with 45 CFR 164.504(e)(2)(ii)(I).
- B. **Termination for Cause.** In accordance with 45 CFR section 164.504(e)(1)(ii), upon CDPH' knowledge of a material breach or violation 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 the Agreement if Business Associate does not cure the breach or end the violation within the time specified by CDPH; or
  2. Immediately terminate the Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.
- C. **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 the Agreement if Business Associate is found guilty of a criminal violation of HIPAA. CDPH may terminate the 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.
- D. **Effect of Termination.** Upon termination or expiration of the 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. If return or destruction is not feasible, Business Associate shall notify CDPH of the conditions that make the return or destruction infeasible, and CDPH and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, 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

Exhibit D  
HIPAA Business Associate Addendum

- 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 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 HITECH Act, 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 HITECH Act, the HIPAA regulations or other applicable laws. CDPH may terminate the 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 the 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 HITECH Act, 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, the HITECH Act 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 VI.D of this Addendum shall survive the termination or expiration of the Agreement.

Exhibit D  
HIPAA Business Associate Addendum

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 Addendum

**Attachment A**  
Business Associate Data Security Requirements

**I. Personnel Controls**

- A. *Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of CDPH, or access or disclose CDPH PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
- B. *Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. *Confidentiality Statement.*** All persons that will be working with CDPH PHI or PI must sign a confidentiality statement that includes, 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 or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for CDPH inspection for a period of six (6) years following contract termination.
- D. *Background Check.*** Before a member of the workforce may access CDPH PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

**II. Technical Security Controls**

- A. *Workstation/Laptop encryption.*** All workstations and laptops that process and/or store CDPH PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDPH Information Security Office.
- B. *Server Security.*** Servers containing unencrypted CDPH PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. *Minimum Necessary.*** Only the minimum necessary amount of CDPH PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. *Removable media devices.*** All electronic files that contain CDPH PHI or PI 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.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.



Exhibit D  
HIPAA Business Associate Addendum

- E. Antivirus software.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- F. Patch Management.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
- G. User IDs and Password Controls.** All users must be issued a unique user name for accessing CDPH PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords 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)
- H. Data Destruction.** When no longer needed, all CDPH PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the CDPH Information Security Office.
- I. System Timeout.** The system providing access to CDPH PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- J. Warning Banners.** All systems providing access to CDPH PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. 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 PI, or which alters CDPH PHI or PI. 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 or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- L. Access Controls.** The system providing access to CDPH PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

Exhibit D  
HIPAA Business Associate Addendum

**M. *Transmission encryption.*** All data transmissions of CDPH PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

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

### III. Audit Controls

**A. *System Security Review.*** All systems processing and/or storing CDPH PHI or PI 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 should include vulnerability scanning tools.

**B. *Log Reviews.*** All systems processing and/or storing CDPH PHI or PI 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 or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

### IV. 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 CDPH PHI or PI 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 the Agreement for more than 24 hours.

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

### V. Paper Document Controls

**A. *Supervision of Data.*** CDPH PHI or PI 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 or PI 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 or PI is contained shall be escorted and CDPH PHI or PI shall be kept out of sight while visitors are in the area.

Exhibit D  
HIPAA Business Associate Addendum

- C. **Confidential Destruction.** CDPH PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. **Removal of Data.** CDPH PHI or PI must not be removed from the premises of the Contractor except with express written permission of CDPH.
- E. **Faxing.** Faxes containing CDPH PHI or PI 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 the fax.
- F. **Mailing.** Mailings of CDPH PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of CDPH PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of CDPH to use another method is obtained.



Karen L. Smith, MD, MPH  
Director and State Health Officer

State of California—Health and Human Services Agency  
California Department of Public Health

Exhibit E



EDMUND G. BROWN JR.  
Governor

**MESSAGE FROM AIDS DRUG ASSISTANCE PROGRAM**

**NOTICE OF PRIVACY PRACTICES**

Effective March 23, 2015

**THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.**

AIDS Drug Assistance Program (ADAP) must keep your health information private. ADAP receives information about you when you apply for benefits and when your pharmacist sends ADAP a bill for your care. ADAP also receives medical information on your treatment when ADAP approves your care. ADAP must give you this notice about the law and how ADAP can use and share your health information and what your rights are.

**HOW ADAP MAY USE AND SHARE INFORMATION ABOUT YOU**

ADAP may only use and share information about you, as required or permitted by law, in the operation of ADAP, Ryan White HIV/AIDS Program, Covered California, and Medi-Cal. This information includes things like your name, address, personal facts, medical history, Social Security Number and medical care given to you.

ADAP uses this information and shares it with others for the following reasons:

- **For payment:** ADAP and others that work with ADAP review, approve, and pay for pharmacy bills sent to ADAP for your medical care. When ADAP does this, ADAP shares information with the pharmacy benefits manager, pharmacists and doctors and others who bill ADAP for your care.
- **For health care operations:** ADAP may use your health records to check the quality of the prescription drug treatment you receive and to check your medical need to

receive restricted ADAP drugs. ADAP may also use this information in audits or fraud investigations, or for planning and managing the ADAP program.

- **Eligibility Determination:** ADAP may share your ADAP information with a Covered California Certified Enrollment Counselor, or with a benefits counselor, case manager, or OA-Health Insurance Premium Payment Program (OA-HIPP) enrollment worker who is an employee or contractor of a Health Insurance and Portability and Accountability Act (HIPAA)-covered county health department delivering HIV or AIDS health care services, for the purpose of enrolling you in and continuing your access to a Medi-Cal or Covered California health plan .

ADAP may also share your name and Social Security Number or individual taxpayer identification number with the Franchise Tax Board. This allows ADAP to verify your income from reported tax records and allows us to obtain required financial documentation if you do not have these records.

## **SOME OTHER WAYS ADAP MAY SHARE YOUR INFORMATION**

The law also allows ADAP to use or give out information ADAP has about you for the following reasons:

- To call or write to you about your benefits with ADAP.
- When required by state or federal law.
- To agencies that oversee audits or investigations for purposes directly related to ADAP.
- In appeals of decisions about health care claims paid or denied by ADAP.
- To the federal government when it is checking on how ADAP is meeting privacy laws.
- To other government agencies that give public benefits such as Medi-Cal, under specified conditions permitted by law.

ADAP may give out health information about you to organizations that help run ADAP's program. If ADAP does, ADAP will make sure that it protects the privacy of your information ADAP shares with them.

Some state laws limit sharing the information listed above. For example, there are special laws, which protect information about HIV/AIDS status, mental health treatment, developmental disabilities, and drug and alcohol abuse care. ADAP will obey these laws.

## **WHEN WRITTEN PERMISSION IS NEEDED**

If ADAP wants to use or give out personal and health information about you for any reason that is not listed above, ADAP must ask your permission in writing. You may take back your written permission at any time, except if we have already acted because of your permission.

## WHAT ARE YOUR PRIVACY RIGHTS UNDER THE LAW?

You have the right to:

- Ask ADAP not to use or share your personal health care information in the ways listed above. However, ADAP may not be able to honor your request.
- Ask ADAP to contact you in writing only or at a different address, post office box, or by telephone. ADAP will accept reasonable requests if needed for your safety.
- To see and get a copy of your ADAP information. You may have someone else see and get a copy of your ADAP information. ADAP has information about your eligibility, your health care bills, and some medical records that ADAP uses to allow or manage your health care services. You will need to pay a fee for ADAP to copy and mail the records. ADAP may keep you from seeing all or parts of your records when the law allows. If ADAP does, ADAP will give you information on how to appeal our decision.
- To change the records if you believe some information ADAP has about you is wrong. ADAP may deny your request if the information was not made or kept by ADAP, or the information is already correct and complete. If your request is denied, you may write a letter disagreeing with ADAP's decision and your letter will be kept with your records.

### \*\*\*\*IMPORTANT\*\*\*\*

**ADAP DOES NOT HAVE COMPLETE COPIES OF YOUR MEDICAL RECORDS. IF YOU WANT TO LOOK AT, GET A COPY OF, OR CHANGE YOUR MEDICAL RECORDS, PLEASE CONTACT YOUR DOCTOR, CLINIC, OR HEALTH CARE PLAN.**

- You have the right to ask for a list of the times when ADAP has shared your health information after April 14, 2003. The list will tell you what information ADAP shared, with whom, when, and for what reasons. The list will not have when ADAP gave information to you, when ADAP had your permission, or when ADAP shared it for treatment, payment, or health care operations.
- You have a right to receive a written copy of this Notice of Privacy Practices when you request it. You can also find this notice on our website at <http://www.cdph.ca.gov/programs/aids/Pages/tOAADAPindiv.aspx>

## HOW DO YOU CONTACT ADAP TO USE YOUR RIGHTS?

Please call or write ADAP if you want to receive the form you will need to exercise your privacy rights.

**ADAP Health Insurance Portability  
and Accountability Act Coordinator**

‰ ADAP

Department of Public Health  
MS 7700, P.O. Box 997426  
Sacramento, CA 95899-7426  
(916) 449-5882

You may also contact your ADAP enrollment worker for the forms necessary to exercise your rights.

If you believe that ADAP has not protected your privacy, you may file a complaint by calling or writing to:

<p style="text-align: center;"><b>Privacy Officer</b> California Department of Public Health Office of Legal Services Privacy Office, 1415 L Street, Suite 500 Sacramento, CA 95814 (916) 440-7671</p>
--

### **COMPLAINTS**

You may also call or write the Secretary of the United States (U.S.), Department of Health and Human Services, Office for Civil Rights, 90 7<sup>th</sup> Street, Suite 4-100, San Francisco, CA 94103, telephone (800) 368-1019 or you may call the U.S. Office for Rights at 866-OCR-PRIV, 866-627-7748, or 866-788-4989 TTY/TDD.

**ADAP cannot take away your health care benefits or retaliate in any way if you file a complaint or use any of the privacy rights in this notice.**

**If you have any questions about this notice, and want more information please contact the California Department of Public Health, Privacy Officer, at the address and telephone number listed above.**

### **CHANGES TO NOTICE OF PRIVACY PRACTICES**

ADAP must obey the rules of this notice. ADAP has the right to make changes in the ADAP privacy rules. If ADAP does make any changes, ADAP will correct this notice and give it to you right away.

To get a copy of this notice in other languages, Braille, large print, audiocassette or computer disk, please call or write to ADAP at the phone number or address listed.

## Exhibit F

### Security Requirements, Protections, and Confidentiality Checklist

Site Name: \_\_\_\_\_ Site Number: \_\_\_\_\_

The Contractor shall complete and return this checklist with the signed copy of the contract agreement. To complete this checklist, the authorized agency administrator or representative attests by checking the boxes adjacent to the statement and signing this checklist that the ADAP Enrollment Site meets, and shall continue to meet throughout the life of the contract (July 1, 2016 – June 30, 2019), the requirements as identified in the Scope of Work which includes those identified below:

1.	The Contractor has reviewed and attests that the contracting agency or organization meets the requirements as written in the "Nondiscrimination Clause (OCP-1)" STD 17A form and has a process in place to deal with discrimination complaints.	
2.	The Contractor can ensure the administrative, physical and technical safeguards of protected health information as required in the CDPH HIPAA BAA 8-14, HIPAA Business Associate Addendum.	
2.a.	<i>Breaches of confidential client information must be immediately reported to CDPH/OA/ADAP. In the space below, please identify the process (and individual/s) your agency or organization has in place to report breaches of ADAP clients' protected health or personal information.</i>	
3.	The ADAP Notice of Privacy Practices is posted in an area at the ADAP Enrollment Site that is accessible and visible to ADAP applicants/clients.	
4.	The Contractor has internet access and scanning and uploading capabilities to allow for the creation of electronic ADAP client files within the designated ADAP's Enrollment Benefits Management secure web-based enrollment system.	
5.	The Contractor has desktop computers with internet access available for all site personnel (shared or individual) who will be performing ADAP enrollment services.	
6.	The Contractor has fax machine/s and scanner/s used to transmit and/or received ADAP client enrollment information/documentation located in a secure area at this ADAP Enrollment Site.	

*All of the requirements listed above must be met in order to become an ADAP Enrollment Site.*

\_\_\_\_\_  
Print Name of Authorized Agency Representative

\_\_\_\_\_  
Title

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date



**Plan for Transporting  
Sample – Confidential ADAP Client Files  
POLICY & PROCEDURE  
[Site Name]**

---

<b>SUBJECT:</b>	Security Policy for Transporting AIDS Drug Assistance Program (ADAP) Enrollment Forms and Documentation	<b>SITE NUMBER:</b>	[XXXX]
<b>REQUESTED BY:</b>	_____	<b>INITIAL REQUEST:</b>	<input type="checkbox"/>
	[Printed Name]	<b>REVISED REQUEST:</b>	<input type="checkbox"/>
	_____	<b>EFFECTIVE DATE:</b>	_____
	[Title]	<b>REVISION DATE:</b>	_____

---

**Background:** [Name of Enrollment Site], AIDS DRUG ASSISTANCE PROGRAM (ADAP), helps to ensure that HIV positive uninsured and under-insured individuals have access to pharmaceutical therapies. The goal of ADAP is to make available, in an effective and timely manner to people living with HIV, drug treatments that can increase the duration and quality of life. In order to serve those in need, it is sometimes necessary to assist individuals with the ADAP eligibility paperwork at an offsite location.

**Purpose:** The purpose of this policy and procedure is to establish guidelines for transporting ADAP enrollment forms and other necessary ADAP client documentation to and from [Name of Enrollment Site], in the event that it is deemed necessary to do the ADAP eligibility paperwork at a location other than at the [Name of Enrollment Site], facility located at [Address of Enrollment Site].

**Policy:** It is the policy of [Name of Enrollment Site], ADAP, to ensure that any transportation of ADAP documentation will be safe, secured and implemented in accordance with [Name of Enrollment Site], guidelines for safeguarding the confidentiality of protected health information. ADAP Enrollment Workers (EWs) will implement reasonable and appropriate administrative, technical, and physical measures to safeguard protected health information from any intentional or unintentional use or disclosure that might violate County, State or Federal privacy regulations, and HIV confidentiality and disclosure laws.

**References:** [Name of Enrollment Site]

[Name of HIPPA document(s) used by site]

[Name of Enrollment Site, Privacy Incident Report]

**Procedure:**

- I. Original client paper records and ADAP enrollment documents **will not** be transported unless necessary to provide services to a client.
- II. It shall be at the discretion of the EWs to determine if it is necessary to transport documents. If deemed necessary:
  - A. An "ADAP Checkout Log" will be completed and maintained by the ADAP Site Contact that includes the ADAP client's name, ADAP documentation transported, date removed, date returned and the EW's name
  - B. All ADAP documents that are transported to an off-site location will be noted on the "ADAP Checkout Log"
  - C. All documentation and records will be returned as quickly as possible
  - D. The "ADAP Checkout Log" will be stored in a confidential and secure location
- III. The safety and return of the documents will be the responsibility of the person who removed them.
- IV. EWs will make every effort to maintain the safety and security of ADAP records when transporting them to or from [Name of Enrollment Site], and completing them at the offsite location.
  - A. ADAP documents will be transported in a folder, inside of a locked brief case, and locked in the vehicle trunk.
  - B. Once ADAP documents have been transported back to the [Name of Enrollment Site], EWs will immediately account for all client documentation and assure that it is returned to its proper, secure destination.
  - C. The use of laptops or other electronic media device to transport documentation is not permitted.

\_\_\_\_\_  
Signature of Site Contact / Agency Administrator

\_\_\_\_\_  
Date Signed

**NONDISCRIMINATION CLAUSE (OCP-1)**

STD. 17A (REV. 9-2000)\_CDPH

1. During the performance of this contract, contractor and its subcontractors shall not unlawfully discriminate, harass or allow harassment against any employee or applicant for employment because of sex, sexual orientation, race, color, religious creed, marital status, denial of family and medical care leave, ancestry, national origin, medical condition (cancer/genetic characteristics), age (40 and above), disability (mental and physical) including HIV and AIDS, denial of pregnancy disability leave or reasonable accommodation. Contractor and subcontractors shall ensure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. Contractor and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Gov. Code, § 12990 et seq.) and the applicable regulations promulgated thereunder (Cal. Code Regs. tit. 2, § 7285.0 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code, § 12990 (a-f), are incorporated into this contract by reference and made a part hereof as if set forth in full (Cal. Code Regs. tit. 2, §7285.0 et seq.). Contractor and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other agreement.
2. This Contractor shall include the non-discrimination and compliance provisions of this clause in all subcontracts to perform work under contract.

**Agreement by Employee/Contractor to Comply with Confidentiality Requirements**

*Summary of Statutes Pertaining to Confidential Public Health Records and Penalties for Disclosure*

All HIV/AIDS case reports and any information collected or maintained in the course of surveillance-related activities that may directly or indirectly identify an individual are considered *confidential public health record(s)* under California Health and Safety Code (HSC), Section 121035(c) and must be handled with the utmost confidentiality. Furthermore, HSC §121025(a) prohibits the disclosure of HIV/AIDS-related public health records that contain any personally identifying information to any third party, unless authorized by law for public health purposes, or by the written consent of the individual identified in the record or his/her guardian/conservator. Except as permitted by law, any person who negligently discloses information contained in a confidential public health record to a third party is subject to a civil penalty of up to \$5,000 plus court costs, as provided in HSC §121025(e)(1). Any person who willfully or maliciously discloses the content of a public health record, except as authorized by law, is subject to a civil penalty of \$5,000-\$25,000 plus court costs as provided by HSC §121025(e)(2). Any willful, malicious, or negligent disclosure of information contained in a public health record in violation of state law that results in economic, bodily, or psychological harm to the person named in the record is a misdemeanor, punishable by imprisonment for a period of up to one year and/or a fine of up to \$25,000 plus court costs (HSC §121025(e)(3)). Any person who is guilty of a confidentiality infringement of the foregoing type may be sued by the injured party and shall be personally liable for all actual damages incurred for economic, bodily, or psychological harm as a result of the breach (HSC §121025(e)(4)). Each disclosure in violation of California law is a separate, actionable offense (HSC §121025(e)(5)).

Because an assurance of case confidentiality is the foremost concern of the California Department of Public Health, Office of AIDS (CDPH/OA), any actual or potential breach of confidentiality shall be immediately reported. In the event of any suspected breach, staff shall immediately notify the director or supervisor of the local health department's HIV/AIDS surveillance unit who in turn shall notify the CDPH/OA Surveillance Section Chief or designee. CDPH/OA, in conjunction with the local health department and the local health officer shall promptly investigate the suspected breach. Any evidence of an actual breach shall be reported to the law enforcement agency that has jurisdiction.

*Employee Confidentiality Pledge*

I recognize that in carrying out my assigned duties, I may obtain access to private information about persons diagnosed with HIV or AIDS that was provided under an assurance of confidentiality. I understand that I am prohibited from disclosing or otherwise releasing any personally identifying information, either directly or indirectly, about any individual named in any HIV/AIDS confidential public health record. Should I be responsible for any breach of confidentiality, I understand that civil and/or criminal penalties may be brought against me. I acknowledge that my responsibility to ensure the privacy of protected health information contained in any electronic records, paper documents, or verbal communications to which I may gain access shall not expire, even after my employment or affiliation with the Department has terminated.

By my signature, I acknowledge that I have read, understand, and agree to comply with the terms and conditions above.

\_\_\_\_\_  
Employee name (print)

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor name (print)

\_\_\_\_\_  
Supervisor Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Name of Employer

PLEASE RETAIN A COPY OF THIS DOCUMENT FOR YOUR RECORDS.