Exhibit A
Scope of Work

1) Service Overview

Contractor agrees to provide to the California Department of Public Health (CDPH) the services described herein.

AIDS Drug Assistance Program (ADAP) and Pre-Exposure Prophylaxis Assistance Program (PrEP-AP) enrollment services, which includes ADAP's Medication Assistance Program and Health Insurance Assistance Programs, and the PrEP-AP.

California Health and Safety Code section (HSC §) §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). HSC § 120972 establishes the PrEP-AP within OA. The AIDS Drug Assistance Program (ADAP) Branch administers both ADAP for people living with HIV and AIDS in California, and PrEP-AP for HIV negative individuals for the prevention of HIV.

2) Service Location

The services shall be performed at Humboldt County DHHS Public Health North Coast AIDS Project, located at:

- 908 7th Street, Eureka, CA 95501

3) Service Hours

The services shall be provided during normal Contractor working hours as defined by the enrollment site.

4) Project Representatives

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

California Department of Public Health	**County of Humboldt**
Sandra Robinson, MBA ADAP Branch Chief Telephone: (916) 449-5942 Fax: (916) 449-5859 E-mail: sandra.robinson@cdph.ca.gov	Michael Weiss, Program Coordinator Telephone: (707) 441-5074 E-mail: mweiss@co.humboldt.ca.us

Exhibit A
Scope of Work

B. Direct all inquiries to:

California Department of Public Health	**County of Humboldt**
PrEP-AP Attention: Jeanene Robinson P.O. Box 997426, MS 7704 Sacramento, CA 95899-7426 Telephone: (916) 445-7572 Fax: (916) 449-5859 E-mail: jeanene.robinson@cdph.ca.gov ADAP Call Center Data Processing Center (CCDPC) Hours: Monday – Friday 8 a.m. to 5 p.m. Telephone: (844) 421-7050 Fax: (844) 421-8008	Attention: Karen Baker, Administrative Analyst 908 7th Street Eureka, CA 95501 Telephone: (707) 441-5575 E-mail: kbaker@co.humboldt.ca.us

C. All payments from CDPH to the Contractor; shall be sent to the following address:

Remittance Address
County of Humboldt
Attention "Cashier": Olivia Wilder, Budget Specialist- DHHS Public Health
Address: 507 F Street Eureka, CA 95501
Phone: (707) 441-5435
Email: owilder@co.humboldt.ca.us

D. 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.

5) Services to be Performed

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

The Contractor Shall:

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
A.1. ES Business Contact Requirement			
Maintain an Enrollment Site (ES) Business Contact to ensure compliance with the requirements of this contract agreement on behalf of the ES and facilitate required information exchange between the ES, CDPH/OA, and CDPH/OA's online ADAP Enrollment System (AES).	Throughout the life of the contract.	ES Administrator	ES Business Contact name and information must be identified in Section 4B. Provide written notice to the assigned CDPH/OA Advisor immediately regarding any changes.
A.2. Nondiscrimination Requirements			
Comply with the provisions as stated in the "Nondiscrimination Clause (STD 17A)", exhibit K. The ES 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.	Throughout the life of the contract.	ES Administrator ES EEO Officer	ES Administrator and/or EEO Officer name and contact information must be identified in Section 4A.
A.3. Information Privacy and Security Requirements			
All personnel conducting enrollment services under this agreement must abide by all applicable laws and CDPH/OA guidelines regarding confidentiality of client eligibility files and protected health information (PHI) when accessing or submitting client data.			
i. Ensure compliance with the provisions as stated in the "HIPAA Business Associate Addendum (CDPH HIPAA BAA 6-16)", exhibit F.	Throughout the life of the contract. Contractor shall also continue to extend the protections of these provisions to PHI upon termination or expiration of the agreement until its	ES Business Contact	Notify the assigned CDPH/OA Advisor immediately by phone call plus email or fax when a potential breach has occurred. EWs may be deactivated if more than two potential breaches occur within a calendar year. An ES may be deactivated if potential breaches are committed by more than two EWs in a calendar year.

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
	return or destruction.		
ii. Ensure that all EWs employed by or volunteering at the ES are issued/assigned an Agency email address. **To ensure client confidentiality, ES staff are prohibited from using a personal email address (i.e. gmail, yahoo, etc.) for CDPH/OA-related correspondence.*	At the time of ES activation and throughout the life of the contract.	ES Administrator ES Business Contact	Verified when EW email address is provided to the assigned CDPH/OA Advisor.
iii. Ensure compliance with the provisions as stated in the applicable "ADAP & PrEP-AP Notice of Privacy Practices", exhibits G & H, and ensure that the notice(s) is posted at the ES.	Throughout the life of the contract.	ES Administrator ES Business Contact	Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", exhibit I. CDPH/OA will verify via visual observation during site visits.
iv. Review and sign the Agreement by Employee/Contractor to Comply with "Confidentiality Requirements (CDPH 8689)", exhibit L.	Annually.	ES Administrator ES Business Contact ES Managers/ Supervisors ES EW(s)	Submit completed form CDPH 8689 via the AES for each staff.
v. Ensure that only certified EWs have access to client eligibility file information, unless otherwise authorized by law.	Throughout the life of the contract.	ES Administrator	Notify the assigned CDPH/OA Advisor immediately by phone call plus email or fax when a potential breach has occurred.

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
** Please refer to the Confidentiality Tables and Information Flows to determine the information sharing requirements that pertain to your ES: https://partners.cdph.ca.gov/sites/ADAPEnrollmentWorkers/*		ES Business Contact	
vi. EWs are required to ask a minimum of three security questions when confirming client identity from an incoming phone call prior to disclosing any PHI.	Throughout the life of the contract.	ES Business Contact ES EW(s)	Notify the assigned CDPH/OA Advisor immediately by phone call plus email or fax when a potential breach has occurred.
vii. EWs are prohibited from disclosing and must employ reasonable measures to protect their EW ID, AES password, or any other identifier/ passcode which may compromise client confidentiality.	Throughout the life of the contract.	ES Business Contact ES EW(s)	Notify the assigned CDPH/OA Advisor immediately by phone call plus email or fax when a potential breach has occurred.
A.4. ES Information Technology/Equipment Requirements			
i. Ensure internet access and equipment and the ability to scan and upload applicant/client eligibility documents to the AES secure enrollment system.	By the go-live date and then throughout the life of the contract.	ES Administrator ES Business Contact	All client enrollments must occur electronically via the AES secure enrollment system.
ii. The use of desktop computers, laptop computers, or other hand held electronic devices for enrollment services must adhere to requirements specified in the “HIPAA Business Associate Addendum (CDPH HIPAA BAA 6-16)”, exhibit F.	By the go-live date and then throughout the life of the contract.	ES Business Contact	Indicate compliance on the “Security Requirements, Protections, and Confidentiality Checklist”, exhibit I.
iii. Ensure that fax machines, printers, scanners, and any other resource equipment that are used to upload and submit client applications or receive	By the go-live date and then throughout the life of the contract.	ES Business Contact	Indicate compliance on the “Security Requirements, Protections, and Confidentiality Checklist”, exhibit I.

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
correspondence which may include confidential client information are located in a secure area.			CDPH/OA will verify via visual observation during site visits.
iv. Ensure use of CDPH-required Multi-Factor Authentication (MFA) when connecting to the AES, such as the Strong Authentication Methods identified in Section 17 of the "CDPH ISO/SR1", exhibit N, or comparable methods. MFA accounts must be individual and unique, not shared by other persons or devices.	By the go-live date and then throughout the life of the contract.	ES Business Contact	Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", exhibit I.
A.5. Quality Requirements			
i. Perform an assessment of service capacity, to confirm that ES staffing is adequate in relation to patient volume. Capacity assessments should be constructed from reasonable projections based on historical enrollments.	By the go-live date.	ES Administrator ES Business Contact	Email a copy of the Service Capacity Assessment to your assigned CDPH/OA Advisor.
ii. In order to ensure adequate service capacity and to maintain a high degree of customer service, ES is required to be adequately staffed during business hours to provide assistance to clients via in-person appointments, secure e-mails, or over the telephone within a reasonable time frame.	Throughout the life of the contract.	ES Administrator ES Business Contact	Failure to maintain adequate service levels may result, at minimum, in CDPH/OA transitioning clients to a neighboring ES.
iii. ES is required to notify CDPH/OA by email at least 2 business days in advance of any known or planned staff absences or site closures (temporary or otherwise) that may impact client services.	Throughout the life of the contract.	ES Administrator ES Business Contact	Notify the assigned CDPH/OA Advisor by email.
iv. ES is required to develop a Contingency Plan for Client Services in the event that the ES has inadequate EW coverage, unplanned closures, or	Throughout the life of the contract.	ES Administrator	Email a copy of the Contingency Plan for Client Services to your assigned CDPH/OA Advisor.

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
an inability to see clients for any time period of more than 4 hours during normal business hours.		ES Business Contact	The plan must include how and to what neighboring ES clients will be redirected.
v. Contracted EW and ES will be held to quality standards and metrics. Please reference the ADAP Resource page found at www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resourcespage.aspx for current year Quality Performance Metrics. CDPH/OA will conduct secondary review on applications. Applications with errors will be considered defective and will count against the performance level of the EW and ES. EW and ES quality will be factored by dividing the number of defective applications by the total number of applications processed.	Throughout the life of the contract.	ES Administrator ES Business Contact	Any continuously deficient EW or ES may be deactivated and precluded from performing CDPH/OA enrollment services. CDPH/OA will continuously monitor performance levels throughout the life of the contract.
A.6. Conduct Requirements			
EWs are required to conduct themselves with a high degree of professionalism and integrity. ES Business Contact is required to ensure that no EW is employed by, nor receives any financial compensation (including gifts or any other type of incentive) from a participating pharmacy and that no client enrollment is conducted at any participating pharmacy location. Additional examples of misconduct include, but are not limited to: i. Knowingly and willfully enrolling clients with inaccurate or false documentation.*	Throughout the life of the contract.	ES Business Contact ES EW(s)	Notify the CDPH/OA Advisor when instances of misconduct are identified. The ES Business Contact may be required to submit a CAP. CDPH/OA staff will address occurrences of misconduct. EWs who engage in misconduct may be subject to temporary or

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
ii. Acting as EW for, or entering AES information in regards to: self, spouse, registered domestic partner, immediate family, or household members. iii. Insubordination and/or non-compliance with CDPH/OA staff requests. iv. Verbal abuse or use of derogatory language. v. Unresponsiveness to CDPH/OA staff and/or client inquiries. vi. Conducting unauthorized off-site client enrollment. vii. Transporting files contrary to, or in absence of, a written transportation plan approved by CDPH/OA. viii. Violating or otherwise not adhering to any requirement stipulated in this scope of work.			permanent suspension of EW status.
** 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.)*			
A.7. Training and Technical Assistance Requirements			
i. Ensure all new EWs have successfully completed new EW training provided by CDPH/OA prior to enrolling or re-certifying clients.	Throughout the life of the contract.	ES Business Contact	Report to the assigned CDPH/OA Advisor, site staff who will be registering for required EW trainings.
ii. Ensure all existing and new EWs complete training on the AES.	Throughout the life of the contract.	ES Business Contact	Report to the assigned CDPH/OA Advisor, site staff who will be registering for required EW trainings.
iii. Ensure compliance with the most recent requirements written in the “California State	Throughout the life of the contract.	ES Business Contact	Report to the assigned CDPH/OA Advisor, site staff who

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
ADAP Guidelines," "California State PrEP-AP Guidelines" and CDPH/OA Management Memos.		ES EW(s)	will be registering for required EW trainings.
iv. Ensure existing EWs maintain active status by participating in required annual recertifying EW trainings and/or other required ad hoc trainings provided by CDPH/OA in order to maintain EW certification to continue conducting client enrollment functions.	Throughout the life of the contract.	ES Business Contact ES EW(s)	Notify EWs to recertify 30 days prior to the recertification end date.
v. Ensure the ES has representation/participation on all monthly CDPH/OA EW calls.	Throughout the life of the contract.	ES Business Contact	Must ensure ES participation for 90 percent of monthly calls. Must contact the CDPH/OA Advisor, if unable to participate on a call to discuss the topics covered.
A.8. Enrollment Tracking Requirements			
i. Ensure all EWs are identified and have a site-specific EW ID number issued by the AES.	Throughout the life of the contract.	ES Business Contact	This site-specific EW ID number may only be used by the EW to whom it is assigned for enrollment activities at this site.
ii. Report any changes in site specific EWs' status (e.g., job duties, relocation, separation, etc.) that will alter the EW(s) ability to enroll clients, including the need for de-activation of any EW ID numbers.	Within 24 hours of the identified change.	ES Business Contact	Report additions/deletions/ changes of EW(s) to the assigned CDPH/OA Advisor.
A.9. Transportation Plan Requirements			
i. Ensure that no client eligibility documentation, records, files, etc., will be transported to or from the ES.	To be maintained throughout the life of the contract.	ES Business Contact	See the "Plan for Transporting Confidential ADAP Client Files", exhibit J.

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
ii. Ensure that no client enrollment files will be transported until CDPH/OA provides written approval of the site's specific transportation plan. Exception to this restriction may be approved by CDPH/OA for the following reasons: i. Client disability; or, ii. Remote distance requires EW to meet with client outside of the ES; or, iii. The entire ES is moving to a new address/location.	30 days prior to the need for transporting any client enrollment documents/files.	ES Business Contact	Submit a written request to the assigned CDPH/OA Advisor which justifies the necessity for transporting client enrollment document/files. The request must also identify the specific procedure to be followed to safeguard the confidentiality of the client documents being transported, as well as who will be responsible/ accountable for site's specific procedure(s). See the "Plan for Transporting Confidential ADAP Client Files", exhibit J.
A.10. Administrative Requirements			
i. Notify the assigned CDPH/OA Advisor if the ES wishes to change from an open site (one which serves any individual who wishes to enroll) to a closed site (one which serves only agency-affiliated individuals) or vice versa.	Provide at least 30-days' notice for the requested change of status.	ES Business Contact	Written request to CDPH/OA Advisor is required (may be submitted by email).
ii. Notify the assigned CDPH/OA Advisor if the ES plans to no longer provide contracted client enrollment services.	At least 60 days prior to planned ES deactivation date.	ES Administrator ES Business Contact	Written Notification required (may be submitted by email) and submission of the "Plan for Transporting Confidential ADAP Client Files", exhibit J, to the site's designated CDPH/OA Advisor assuring the secure transfer of hard copy client files.
iii. Ensure that clients are made aware of, and have access to, the CDPH/OA program brochures and	By the go-live date and then	ES Business Contact	CDPH/OA will verify, via review of the CDPH/OA Client

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
info sheets. Copies of the most recent brochures and info sheets must be located in an area of the ES that is visible to clients.	throughout the life of the contract.		Satisfaction Survey, and via visual observation during site visits.
A.11. ADAP Fiscal Requirements			
i. Ensure CDPH/OA funds are used exclusively to cover costs related to ADAP in accordance with HSC §120956(b).	Throughout the life of the contract. Within five business days of request.	ES Administrator ES Business Contact	Within five business days, upon request, submit to CDPH/OA for review budget and expense reports with sufficient detail to ensure compliance with section A.11. In the event of an audit or upon request by CDPH/OA, ES must be able to adequately show that these contractual requirements have been met.
ii. Ensure compliance with the federal Health Resources and Services Administration Ryan White HIV/AIDS Program requirements, policies, and National Monitoring Standards.	Throughout the life of the contract. Within five business days of request.	ES Administrator ES Business Contact	Within five business days, upon request, submit to CDPH/OA for review budget and expense reports with sufficient detail to ensure compliance with section A.11. In the event of an audit or upon request by CDPH, ES must be able to adequately show that these contractual requirements have been met.
iii. Ensure funds received from CDPH/OA are not used for unallowable expenses as defined by the Ryan White National Monitoring Standards.	Throughout the life of the contract.	ES Administrator	Within five business days, upon request, submit to CDPH/OA for review budget and expense

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
	Within five business days of request.	ES Business Contact	reports with sufficient detail to ensure compliance with section A.11. In the event of an audit or upon request by CDPH, ES must be able to adequately show that these contractual requirements have been met.
A.12. PrEP-AP Fiscal Requirements			
i. Ryan White funds are prohibited for the use of PrEP-AP enrollment services.	Throughout the life of the contract. Within 15 business days.	ES Administrator ES Business Contact	Within 15 business days, upon request, ES is required to submit documentation of all EWs performing PrEP enrollment with a budget detail indicating how each EW is funded.
ii. EWs who conduct PrEP-AP enrollment are precluded from being 100 percent funded by Ryan White funds.	Throughout the life of the contract. Within 15 business days.	ES Administrator ES Business Contact	Within 15 business days, upon request, ES is required to submit documentation of all EWs performing PrEP-AP enrollment with an itemized budget detail detailing how each EW is funded.
A.13. Auditing Requirements			
i. Facilitate CDPH/OA site visit requests, including but not limited to receiving or providing required documentation/information as requested by the assigned CDPH/OA Advisor. Act as liaison between the site, CDPH/OA Advisor, EW(s), and the ADAP Coordinator within the Local Health	As needed during normal working hours throughout the life of the contract.	ES Administrator ES Business Contact	Respond to written notifications and requests for information initiated by CDPH/OA personnel.

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
Jurisdiction (if applicable) regarding activities related to the site visit.			
ii. Ensure that CDPH/OA staff, authorized CDPH/OA representatives and/or other state and federal agencies are granted access to all client eligibility files and any other documentation related to this contract agreement for audit purposes.	As needed during normal working hours throughout the life of the contract.	ES Administrator ES Business Contact	Within five business days, respond to written and in-person requests for client files made by CDPH/OA staff.
iii. Develop and submit required Corrective Action Plan (CAP) when required based on results of site visit/federal or state program audit of grievance reports filed against the EW or ES.	As needed.	ES Administrator ES Business Contact	CAP is to be submitted to the assigned CDPH/OA Advisor by the timeframe identified in the letter indicating the CAP is required.
iv. All client information must be uploaded securely to the AES. ES is not required to maintain paper-based client files for active clients. Maintain existing hard copy client files/records for four years. Once these files have reached the retention timeframe, they may be destroyed. Continuing to maintain paper files is optional, but must follow the document retention timeframe.	Throughout the life of the contract.	ES Business Contact	As needed, records will be made available to view within the timeframe provided by the federal or state auditors. At contract termination or expiration, documents containing PHI must be returned or retained in accordance with the “HIPAA Business Associate Addendum” (CDPH HIPAA BAA 6-16), exhibit F.
A.14. Grievance Requirements			
i. Ensure that clients are made aware of, and have access to, the CDPH/OA grievance procedures and Medication and Insurance Assistance	Upon initial and annual re-enrollments of ADAP clients and	ES Business Contact ES EW(s)	CDPH/OA will verify, via review of the CDPH/OA Client Satisfaction Survey, and via

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
Programs Grievance Form as outlined in the California State ADAP/PrEP-AP Guidelines. Copies of the Medication and Insurance Assistance Programs Grievance Form must be located in an area of the ES that is visible to clients.	annual re-enrollment of PrEP-AP clients.		visual observation during site visits. Indicate compliance on the "Security Requirements, Protections, and Confidentiality Checklist", exhibit I.
ii. Upon client request, assist clients in the completion and submission of a Medication and Insurance Assistance Programs Grievance Form and related documents. Assistance may also include providing the mailing address and contact information for CDPH/OA Advisors and/or other CDPH/OA Contractors, and/or the submission of the completed grievance form and related documents to CDPH/OA.	As needed.	ES Business Contact ES EW(s)	Notify the ADAP Call Center Data Processing Center (CCDPC) immediately if assistance is needed with the CDPH/OA grievance process.
A.15. Performance Requirements			
i. EWs are required by law to vigorously pursue enrollment into health care coverage for which clients may be eligible (e.g., Medicaid, Medicare, employer-sponsored health insurance coverage, and/or other private health insurance) to comply with federal and state payer of last resort requirements.	Throughout the life of the contract.	ES Business Contact ES EW(s)	Upon initial enrollment and annual re-enrollment. EWs are required to assess client's eligibility for other third-party coverage based on eligibility documents provided. All eligible individuals must apply.
ii. EWs are required to proactively conduct outreach to clients, by utilizing the AES dashboard to identify clients who have an eligibility expiration date within 30 days. EWs must document the client outreach in the case notes.	Throughout the life of the contract.	ES Business Contact ES EW(s)	Outreach attempts and any client interaction as a result of said outreach must be clearly documented in the client case notes available through AES.

Exhibit A
Scope of Work

Enrollment Site Requirements	Time Line	Responsible Party	Performance Measure and/or Deliverables
iii. PrEP-AP EWs are required to enroll eligible clients in the appropriate medication manufacturer assistance program when performing enrollment and re-enrollment to comply with payer of last resort requirements.	Throughout the life of the contract.	ES Business Contact ES EW(s)	Upon initial enrollment and annual re-enrollment. EWs are required to assess client's eligibility for medication manufacturer assistance program(s) based on eligibility documents provided. All eligible individuals must apply.
iv. If the ES is also a contracted clinical site in the PrEP-AP Clinical Provider Network, PrEP-AP EWs are required to perform a warm handoff to clients being clinically assessed for PrEP clinical eligibility after the client has been enrolled in the PrEP-AP and manufacturer assistance program.	Throughout the life of the contract.	ES Business Contact PrEP-AP EW(s)	Activities must be clearly documented in the client case notes available through AES.
v. For clients who test HIV-positive when undergoing an initial assessment for PrEP clinical eligibility or who seroconvert while enrolled in the PrEP-AP, PrEP-AP EWs are required, **within forty-eight hours** of notification of HIV positive status, to: a) refer PrEP-AP clients to an authorized ADAP ES, or b) provide clients with contact information to the CCDPC to be linked to an ADAP ES	Throughout the life of the contract.	ES Business Contact PrEP-AP EW(s)	Activities must be clearly documented in the client case notes available through AES.

Exhibit A, Attachment I
Definition of Terms

Item	Definition
AIDS Drug Assistance Program (ADAP)	Federally funded program that helps ensure that people living with HIV/AIDS who are uninsured and under-insured have access to life-saving medications on the ADAP formulary through medication and health insurance assistance programs. ADAP provides assistance with medication, health insurance premium payments, and medical out of pocket payments.
ADAP and PrEP-AP Benefits	Benefits available for eligible Clients who enroll in a CDPH/OA program. These services can include: • Formulary medication assistance • Prescription Claim third party insurance copays, deductibles, and co-insurance • Medi-Cal Prescription Claim share of cost • Outpatient Medical Out of Pocket Cost reimbursements • Private health insurance premium payments • Medicare Part D premium payments • Medigap premium payments • PEP starter packs • PrEP starter packs • HIV Testing • STI Testing • Pregnancy Testing • Renal Function Testing • Hepatitis A, B, and/or C Screenings
ADAP and PrEP-AP Data	The information collected and used by CDPH/OA, Providers, ADAP Enrollment Sites, and any other entity associated with the delivery of ADAP or PrEP-AP Benefits for the purpose of administering the ADAP program. ADAP Data includes: (1) Client eligibility and enrollment information, (2) Information identifying CDPH/OA authorized enrollment sites and workers, (3) Prescription, dispensing, premiums, billing information, and Outpatient Medical Out of Pocket Costs, and (4) all other data pertaining to this Agreement. Data is a set of values of qualitative or quantitative variables; restated, pieces of data are individual pieces of information. Data is measured, collected and reported, and analyzed, whereupon it can be visualized using graphs or images.

Exhibit A, Attachment I
Definition of Terms

Item	Definition
ADAP Coordinator	Local agency staff designated to act as the primary county contact between the CDPH/OA enrollment sites, OA, and CDPH/OA contractors
ADAP Enrollment System (AES)	Online system used by certified CDPH/OA and Contractor staff to enroll/re-enroll/recertify clients into any of the CDPH/OA medication and insurance assistance programs.
Administration Costs	Subrecipient administrative activities such as: Usual and recognized overhead activities, including established indirect costs; Management oversight of specific programs funded under the RWHAP; and other types of program support such as quality assurance, quality control, and related activities (exclusive of RWHAP CQM).
Agreement	A negotiated and legally binding arrangement between parties as to a course of action.
Business Days	Monday through Friday, excluding Thanksgiving, Christmas, and New Year's Day.
California Department of Public Health (CDPH)	The lead agency in California providing detection, treatment, prevention, and surveillance of public health issues.
California Department of Public Health Office of AIDS (CDPH/OA)	The organizational level within CDPH that has overarching responsibility for HIV medication and insurance assistance programs, including the AIDS Drug Assistance Program, Pre-Exposure Prophylaxis Assistance Program, Employer-Based Health Insurance Premium Payments Program, Medicare Part D Premium Payments Program, and Office of AIDS Health Insurance Premium Payments Program.
CDC Guidelines	The most recent recommendations on preexposure or postexposure prophylaxis published by the federal Centers for Disease Control and Prevention (CDC).
CDPH Guidelines	Guidelines include all policy, procedures, and management memos made known by CDPH/OA. Current guidelines are

Exhibit A, Attachment I
Definition of Terms

Item	Definition
	located on the OA website at: https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_communications.aspx.
Centers for Medicare and Medicaid Services (CMS)	The US federal agency that administers Medicare, Medicaid, and the State Children's Health Insurance Program, among others.
Client	May mean either of the following: a) Individuals enrolled in ADAP and eligible for ADAP services who meet the following criteria: 1. are HIV infected; 2. are a resident of California; 3. are 18 years of age or older; 4. are enrolled in the medication manufacturer's assistance program (if eligible); 5. have an annual MAGI that does not exceed 500% of the FPL based on family size and household income; and 6. are not fully covered by or eligible for Medi-Cal or other third-party payers. b) Individuals enrolled in PrEP-AP and eligible for PrEP-AP services who meet the following criteria: 1. are a resident of California; 2. have a negative HIV/AIDS test result (dated within 6 months of the PrEP-AP application); 3. are 18 years of age or older; 4. have an annual MAGI that does not exceed 500% of the FPL based on family size and household income; 5. are not fully covered by or eligible for Medi-Cal or other third party payers; and 6. are enrolled in the medication manufacturer's assistance program (if eligible).
Closed Site	ADAP enrollment site that only serves ADAP applicants/clients receiving medical care at their facility. (see also: Open Site)

Exhibit A, Attachment I
Definition of Terms

Item	Definition
Community-Based Organization (CBO)	Non-profit 501(c)(3) entities that operate within a single local community.
Contract Year	Twelve month periods from the anniversary of the End Date.
Contractor	The entity awarded the Agreement identified on the STD 213.
Deductible	The amount a client owes for covered prescription services before their health insurance plan will pay.
Dispense Fee	The amount reimbursed to a pharmacy when filling a prescription to cover the charge for professional services and overhead costs.
Effective Date	The date this Agreement becomes effective as listed on the STD 213 of this Agreement.
Eligibility Documents	Documents used by CDPH/OA to establish Client eligibility for program benefits. These documents include but are not limited to ADAP/PrEP-AP applications, recertification forms, initial diagnosis verification, proof of identity, proof of income, proof of State residency, copies of recent CD4 and viral load lab results. If applicable, proof of Medi-Cal application, proof of Medi-Cal ineligibility, dependent verification, Medicare Part D documents (e.g., letter of creditable coverage, future eligibility or eligibility termination), copies of health care coverage cards, and recent premium and billing statements.
Emergency Access	A process that ensures that ADAP clients have continuous access to their life-saving treatment. Allows expeditious access to ADAP formulary medications for ADAP clients who do not have access to ADAP medications and are at risk for a treatment interruption.
Employer-Based Health Insurance Premium Payment (EB-HIPP)	A subsidy program that provides premium assistance for an ADAP client's portion of their employer-based insurance premiums. Individuals enrolled in EB-HIPP are also eligible for the medical out-of-pocket benefit.

Exhibit A, Attachment I
Definition of Terms

Item	Definition
End Date	The date this Agreement terminates as listed on the STD 213 of this Agreement.
Enrollment site (ES)	A physical location that provides client enrollment services for any of the contractually authorized CDPH/OA programs. ES are limited to community-based non-profit organizations, clinics, medical providers, and case management service providers including counties or local health jurisdictions/departments (LHJ).
ES Business Contact	Contractor's primary administrative contact who is dedicated to overseeing the Agreement. Acts as the primary contact between OA, the ADAP Coordinator within the LHJ, and CDPH/OA service contractors. This staff person may not also be an active EW.
Enrollment Worker (EW)	Contracted ES staff that are certified and trained to assist eligible clients with enrollment, reenrollment, and recertification in CDPH/OA medication and insurance assistance programs. EWs must attend an initial web-based training, and recertify annually through a web-based training provided by CDPH/OA.
ePrescribing	Abbreviation for electronic prescribing referring to the use of technology such as a computer or wireless device to write and transmit a prescription directly to a pharmacy. May include clinical and cost information.
Execution Date	The date the Agreement is signed by CDPH/OA.
Federal Poverty Level (FPL)	Income level is determined by the federal Department of Health and Human Services to represent poverty. FPL varies according to family size and changes yearly.
Fiscal Year (FY)	State of California fiscal year, July 1 through June 30 annually.
Formulary	Defined in California Health and Safety code section 120955(a)(2): The director, in consultation with the ADAP Medical Advisory Committee, shall develop, maintain, and update as necessary a list of drugs to be provided under this program.

Exhibit A, Attachment I
Definition of Terms

Item	Definition
	ADAP's formulary is located at CDPH/OA web page: https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resourcespage.aspx. PrEP-AP's formulary is located at CDPH/OA webpage: https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resources_prepAP.aspx
Go Live Date	The date Participating Entities begin receiving products and services through the Agreement.
Health Insurance Portability and Accountability Act (HIPAA)	The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 as amended, and the regulations promulgated thereunder.
Health Resources and Services Administration (HRSA)	The Federal agency that administers Ryan White funding.
Insurance Benefits Manager (IBM)	Service contractor that manages and processes health insurance premium payments for clients enrolled in CDPH/OA's medication and insurance assistance programs.
Local Health Jurisdiction/ Department (LHJ)	One of 58 counties and three cities (Pasadena, Long Beach, and Berkeley) in the state of California authorized to act as a local governmental public health presence.
Medical Advisory Committee (MAC)	An advisory body to CDPH/OA and consists of physicians, pharmacists, health professionals, and community members who review the Formulary and make recommendations for additions, deletions, or other changes to the Formulary.
Medical Benefit Manager (MBM)	Service contractor that manages and processes outpatient medical out of pocket payments for clients enrolled in CDPH/OA's medication and insurance assistance programs.

Exhibit A, Attachment I
Definition of Terms

Item	Definition
Medical Out of Pocket Costs (MOOP) benefit	For eligible clients enrolled in any of CDPH/OA's premium assistance programs, covers outpatient medical out-of-pocket costs that count towards the client's health insurance policy's annual out of pocket maximum. May include copayments, deductibles, coinsurance, share of costs, and other specific expenses.
Medi-Cal Share of Cost	The monthly amount of medical expenses, including prescriptions, a Medi-Cal beneficiary with a share of cost obligation must incur before they are eligible to receive Medi-Cal benefits.
Medicare Part D Premium Payment Program (MDPP)	Subsidy program that pays Medicare Part D and Medigap insurance premiums for individuals who are enrolled in ADAP and a Medicare Part D prescription drug plan. Individuals that are enrolled in MDPP are also eligible for the MOOP benefit.
Medication Assistance Program (MAP)	The ADAP MAP pays for the prescription costs of medication on the ADAP Formulary for eligible individuals.
Modified Adjusted Gross Income (MAGI)	As defined in Health and Safety Code section 120960(i)(5), MAGI is based on federal Internal Revenue Code which includes Federal Adjusted Gross Income (FAGI) plus the following income if applicable: a) non-taxable Social Security benefits which includes disability payments (SSDI) but does not include Supplemental Security Income (SSI), b) tax-exempt interest, and, c) excluded foreign earned income and housing expenses for Americans living abroad.
Multi-Factor Authentication (MFA)	An authentication method in which an authorized user is granted individual access to the AES only after successfully presenting two or more pieces of evidence to an authentication mechanism. This additional layer of security and verification is to ensure the protection of client data.

Exhibit A, Attachment I
Definition of Terms

Item	Definition
National Drug Code (NDC)	The NDC is a unique 11-digit, 3-segment number which identifies the labeler, product, and trade package size. The first segment, the labeler code, is assigned by the FDA. A labeler is any firm that manufactures (including repackagers or relabelers), or distributes (under its own name) the drug. The second segment, the product code, identifies a specific strength, dosage form, and formulation for a particular firm. The third segment, the package code, identifies package sizes and types. Both the product and package codes are assigned by the firm. For purposes of this contract the NDC shall be reported in the 11-digit format 5-4-2.
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.
OA Advisor	OA staff assigned to a LHJ or ES for monitoring and technical assistance.
Office of AIDS-Health Insurance Premium Payment (OA-HIPP)	Program that pays for private health insurance premiums and medical out of pocket costs for clients co-enrolled in ADAP's medication assistance program.
Open Site	ES that will assist applicants/clients irrespective of where they receive their medical care. (see also: Closed Site)
Payer of Last Resort	The state and federal requirement that Ryan White services are billed after the primary payers have been billed. May also be written as Payor of Last Resort.
PEP starter packs	An initial supply of PEP medication.
Pharmacy Benefit Manager (PBM)	Service contractor administering the ADAP statewide pharmacy network and providing pharmaceutical services for CDPH/OA clients.
Pharmacy Provider Network	The pharmacies subcontracted with the Contractor to dispense drugs on the ADAP and/or PrEP-AP formulary to Clients.

Exhibit A, Attachment I
Definition of Terms

Item	Definition
Post-Exposure Prophylaxis (PEP)	A fixed-dose combination of tenofovir disoproxil fumarate (TDF) and emtricitabine (FTC) with integrase or protease inhibitors, or another drug or drug combination that meets the same clinical eligibility recommendations provided in CDC guidelines.
Pre-Exposure Prophylaxis (PrEP)	A fixed-dose combination of TDF with FTC, or another drug or drug combination that meets the same clinical eligibility recommendations provided in CDC guidelines.
PrEP Assistance Program (PrEP-AP)	PrEP-AP provides assistance with PrEP-related medical out-of-pocket costs and access to medications on the PrEP-AP formulary for the prevention of HIV and treatment of sexually transmitted infections. The PrEP-AP provides assistance to both uninsured and insured individuals at risk for, but not infected with HIV.
PrEP starter packs	An initial supply of PrEP medication.
Prescription Claims	Claims for outpatient prescription drugs on the Formulary dispensed to Clients.
Protected Health Information (PHI)	Information that identifies, or can be used to identify, an individual. PHI contains information that relates to the past, present or future health condition of an individual patient in any form, including paper, electronic, and oral communications as defined by the Health Insurance Portability and Accountability Act
Provider	Persons that provide health or health-related services to Clients; includes EWs, case managers, pharmacists, medical providers, insurance plans or administrators, and physicians.
Rapid ART	Rapid or immediate initiation of antiretroviral therapy (ART), with the goals of providing Intake, first care appointment, and ART initiation within 5 days of new HIV diagnosis.
Recognized Holidays	Christmas, Thanksgiving, and New Year's Day.

Exhibit A, Attachment I
Definition of Terms

Item	Definition
State	For the purposes of this Agreement, refers to CDPH/OA.
Telemedicine	Telemedicine is the use of telecommunication and information technology to provide clinical services from a distance. CDPH/OA contracts to provide telemedicine services to PrEP-AP clients for PrEP- and PEP-related medical services. This allows PrEP-AP clients to access PrEP-related clinical services from the comfort of their own home using a mobile device.
Temporary Access Period (TAP)	An approved TAP grants an applicant 30 days of temporary ADAP eligibility in which to obtain and submit required documentation to a certified ADAP enrollment worker so as to substantiate program eligibility.
Third Party Payer	Any private, state, or federal program that provides reimbursement to health care providers for prescriptions and medical services rendered to a Client, examples include but are not limited to Medi-Cal (the State of California Medicaid), Medicare, private health insurance.

Exhibit B
Budget Detail and Payment Provisions

1. Invoicing and Payment

A. In no event shall the Contractor request reimbursement from the State for obligations entered into or for costs incurred 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 System (AES) 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

Enrollment sites will be paid a fee for services performed, calculated on current client enrollment data as provided by AES to determine the number of program services provided at each enrollment site. Services must be complete with all required forms and verifying documentation.

Exhibit B
Budget Detail and Payment Provisions

The following documents and any subsequent updates are not attached but are incorporated herein and made a part hereof by this reference. CDPH will maintain on file, all documents referenced herein and any subsequent updates, as required by program directives. CDPH shall provide the Contractor with copies of said documents and any periodic updates thereto, under separate cover.

AIDS Drug Assistance Program Enrollment Site Fee for Service Pay Schedule, located at in the Reference Guides page listed as Enrollment Site Fee Schedule in the attached link below:
https://www.cdph.ca.gov/programs/cid/doa/pages/oa_adap_resourcespage.aspx

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 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 fiscal year 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 Contractor to reflect the reduced amount.

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 Submission of Final Invoice

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 enrollment 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/PrEP-AP enrollment services (as verified by CDPH/OA/ADAP through the AES 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

D. The Contractor is hereby advised of its obligation to submit to the state a completed copy of the **"Contractor's Release (Exhibit O)".**

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.

B. 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.

6. Travel and Per Diem Reimbursement

No travel shall be permitted under this agreement.

Exhibit D
Special Terms and Conditions

(For Subvention/Local Assistance Agreements)

The provisions herein apply to this Agreement unless the provisions are removed by reference, the provisions are superseded by an alternate provision appearing elsewhere in this Agreement, or the applicable conditions do not exist.

Index of Special Terms and Conditions

1. Procurement Rules
2. Equipment Ownership / Inventory / Disposition
3. Subcontract Requirements
4. Income Restrictions
5. Site Inspection
6. Intellectual Property Rights
7. Prior Approval of Training Seminars, Workshops or Conferences
8. Confidentiality of Information
9. Documents, Publications, and Written Reports
10. Dispute Resolution Process
11. Officials Not to Benefit
12. Prohibited Use of State Funds for Software
13. Contract Uniformity (Fringe Benefit Allowability)
14. Cancellation

1. Procurement Rules

(Applicable to all agreements in which equipment, property, commodities and/or supplies are furnished by CDPH or expenses for said items are reimbursed with state or federal funds.)

a. **Equipment definitions**

Wherever the term equipment /property is used, the following definitions shall apply:

(1) **Major equipment/property**: A tangible or intangible item having a base unit cost of **$5,000 or more** with a life expectancy of one (1) year or more and is either furnished by CDPH or the cost is reimbursed through this Agreement. Software and videos are examples of intangible items that meet this definition.

(2) **Minor equipment/property**: A tangible item having a base unit cost of **less than $5,000** with a life expectancy of one (1) year or more and is either furnished by CDPH or the cost is reimbursed through this Agreement.

b. **Government and public entities** (including state colleges/universities and auxiliary organizations), whether acting as a contractor, may secure all commodities, supplies, equipment and services related to such purchases that are required in performance of this Agreement. Said procurements are subject to Paragraphs d through g of this provision. Paragraph c of this provision shall also apply, if equipment purchases are delegated to subcontractors that are nonprofit organizations or commercial businesses.

c. **Nonprofit organizations and commercial businesses**, whether acting as a contractor and/or subcontractor, may secure commodities, supplies, equipment and services related to such purchases for performance under this Agreement.

(1) Equipment purchases shall not exceed $50,000 annually.

To secure equipment above the annual maximum limit of $50,000, the Contractor shall make arrangements through the appropriate CDPH Program Contract Manager, to have all remaining equipment purchased through CDPH's Purchasing Unit. The cost of equipment purchased by or through CDPH shall be deducted from the funds available in this Agreement. Contractor shall submit to the CDPH Program Contract Manager a list of equipment specifications for those items that the State must procure. The State may pay the vendor directly for such arranged equipment purchases and title to the equipment will remain with CDPH. The equipment will be delivered to the Contractor's address, as stated on the face of the Agreement, unless the Contractor notifies the CDPH Program Contract Manager, in writing, of an alternate delivery address.

(2) All equipment purchases are subject to paragraphs d through g of this provision. Paragraph b of this provision shall also apply, if equipment purchases are delegated to subcontractors that are either a government or public entity.

(3) Nonprofit organizations and commercial businesses, shall use a procurement system that meets the following standards:

(a) Maintain a code or standard of conduct that shall govern the performance of its officers,

employees, or agents engaged in awarding procurement contracts. No employee, officer, or agent shall participate in the selection, award, or administration of a procurement, or bid contract in which, to his or her knowledge, he or she has a financial interest.

(b) Procurements shall be conducted in a manner that provides, to the maximum extent practical, open, and free competition.

(c) Procurements shall be conducted in a manner that provides for all of the following:

[1] Avoid purchasing unnecessary or duplicate items.

[2] Equipment solicitations shall be based upon a clear and accurate description of the technical requirements of the goods to be procured.

[3] Take positive steps to utilize small and veteran owned businesses.

d. Unless waived or otherwise stipulated in writing by CDPH, prior written authorization from the appropriate CDPH Program Contract Manager will be required before the Contractor will be reimbursed for any purchase **exceeding** $2,500 or more for commodities, supplies, equipment, and services related to such purchases. The Contractor must provide in its request for authorization all particulars necessary, as specified by CDPH, for evaluating the necessity or desirability of incurring such costs. The term "purchase" excludes the purchase of services from a subcontractor and public utility services at rates established for uniform applicability to the general public.

e. In special circumstances, determined by CDPH (e.g., when CDPH has a need to monitor certain purchases, etc.), CDPH may require prior written authorization and/or the submission of paid vendor receipts for any purchase, regardless of dollar amount. CDPH reserves the right to either deny claims for reimbursement or to request repayment for any Contractor purchase that CDPH determines to be unnecessary in carrying out performance under this Agreement.

f. The Contractor must maintain a copy or narrative description of the procurement system, guidelines, rules, or regulations that will be used to make purchases under this Agreement. The State reserves the right to request a copy of these documents and to inspect the purchasing practices of the Contractor at any time.

g. For all purchases, the Contractor must maintain copies of all paid vendor invoices, documents, bids and other information used in vendor selection, for inspection or audit. Justifications supporting the absence of bidding (i.e., sole source purchases) shall also be maintained on file by the Contractor for inspection or audit.

2. Equipment Ownership / Inventory / Disposition

(Applicable to agreements in which equipment and/or property is furnished by CDPH and/or when said items are purchased or reimbursed with state)

a. Wherever the terms equipment and/or property are used in this provision, the definitions in provision 1, paragraph a., shall apply.

Unless otherwise stipulated in this Agreement, all equipment and/or property that are

purchased/reimbursed with agreement funds or furnished by CDPH under the terms of this Agreement shall be considered state equipment and the property of CDPH.

(1) CDPH requires the reporting, tagging and annual inventorying of all equipment and/or property that is furnished by CDPH or purchased/reimbursed with funds provided through this Agreement.

Upon receipt of equipment and/or property, the Contractor shall report the receipt to the CDPH Program Contract Manager. To report the receipt of said items and to receive property tags, Contractor shall use a form or format designated by CDPH's Asset Management Unit. If the appropriate form (i.e., Contractor Equipment Purchased with CDPH Funds) does not accompany this Agreement, Contractor shall request a copy from the CDPH Program Contract Manager.

(2) If the Contractor enters into an agreement with a term of more than twelve months, the Contractor shall submit an annual inventory of state equipment and/or property to the CDPH Program Contract Manager using a form or format designated by CDPH's Asset Management Unit. If an inventory report form (i.e., Inventory/Disposition of CDPH-Funded Equipment) does not accompany this Agreement, Contractor shall request a copy from the CDPH Program Contract Manager. Contractor shall:

(a) Include in the inventory report, equipment and/or property in the Contractor's possession and/or in the possession of a subcontractor (including independent consultants).

(b) Submit the inventory report to CDPH according to the instructions appearing on the inventory form or issued by the CDPH Program Contract Manager.

(c) Contact the CDPH Program Contract Manager to learn how to remove, trade-in, sell, transfer or survey off, from the inventory report, expired equipment and/or property that is no longer wanted, usable or has passed its life expectancy. Instructions will be supplied by CDPH's Asset Management Unit.

b. Title to state equipment and/or property shall not be affected by its incorporation or attachment to any property not owned by the State.

c. Unless otherwise stipulated, CDPH shall be under no obligation to pay the cost of restoration, or rehabilitation of the Contractor's and/or Subcontractor's facility which may be affected by the removal of any state equipment and/or property.

d. The Contractor shall maintain and administer a sound business program for ensuring the proper use, maintenance, repair, protection, insurance and preservation of state equipment and/or property.

(1) In administering this provision, CDPH may require the Contractor to repair or replace, to CDPH's satisfaction, any damaged, lost or stolen state equipment and/or property. Contractor shall immediately file a theft report with the appropriate police agency or the California Highway Patrol and Contractor shall promptly submit one copy of the theft report to the CDPH Program Contract Manager.

e. Unless otherwise stipulated by the program funding this Agreement, equipment and/or property purchased/reimbursed with agreement funds or furnished by CDPH under the terms of this

Agreement, shall only be used for performance of this Agreement or another CDPH agreement.

f. Within sixty (60) calendar days prior to the termination or end of this Agreement, the Contractor shall provide a final inventory report of equipment and/or property to the CDPH Program Contract Manager and shall, at that time, query CDPH as to the requirements, including the manner and method, of returning state equipment and/or property to CDPH. Final disposition of equipment and/or property shall be at CDPH expense and according to CDPH instructions. Equipment and/or property disposition instructions shall be issued by CDPH immediately after receipt of the final inventory report. At the termination or conclusion of this Agreement, CDPH may at its discretion, authorize the continued use of state equipment and/or property for performance of work under a different CDPH agreement.

g. **Motor Vehicles**

(Applicable only if motor vehicles are purchased/reimbursed with agreement funds or furnished by CDPH under this Agreement.)

(1) If motor vehicles are purchased/reimbursed or furnished by CDPH under the terms of this Agreement, within thirty (30) calendar days prior to the termination or end of this Agreement, the Contractor shall return such vehicles to CDPH and shall deliver all necessary documents of title or registration to enable the proper transfer of a marketable title to CDPH.

(2) If motor vehicles are purchased/reimbursed or furnished by CDPH under the terms of this Agreement, ***the State of California shall be the legal owner of said motor vehicles and the Contractor shall be the registered owner***. The Contractor shall only use said vehicles for the performance under the terms of this Agreement.

(3) The Contractor agree that all operators of motor vehicles, purchased/reimbursed or furnished by CDPH under the terms of this Agreement, shall hold a valid State of California driver's license. In the event that ten or more passengers are to be transported in any one vehicle, the operator shall also hold a State of California Class B driver's license.

(4) If any motor vehicle is purchased/reimbursed or furnished by CDPH under the terms of this Agreement, the Contractor, as applicable, shall provide, maintain, and certify that, at a minimum, the following type and amount of automobile liability insurance is in effect during the term of this Agreement or any extension period during which any vehicle remains in the Contractor's possession:

Automobile Liability Insurance

(a) The Contractor, by signing this Agreement, hereby certifies that it possesses or will obtain automobile liability insurance in the amount of $1,000,000 per occurrence for bodily injury and property damage combined. Said insurance must be obtained and made effective upon the delivery date of any motor vehicle, purchased/reimbursed with agreement funds or furnished by CDPH under the terms of this Agreement, to the Contractor.

(b) The Contractor shall, as soon as practical, furnish a copy of the certificate of insurance to the CDPH Program Contract Manager. The certificate of insurance shall identify the CDPH contract or agreement number for which the insurance applies.

(c) The Contractor agree that bodily injury and property damage liability insurance, as required herein, shall remain in effect at all times during the term of this Agreement or until such time as the motor vehicle is returned to CDPH.

(d) The Contractor agree to provide, at least thirty (30) days prior to the expiration date of said insurance coverage, a copy of a new certificate of insurance evidencing continued coverage, as indicated herein, for not less than the remainder of the term of this Agreement, the term of any extension or continuation thereof, or for a period of not less than one (1) year.

(e) The Contractor, if not a self-insured government and/or public entity, must provide evidence, that any required certificates of insurance contain the following provisions:

[1] The insurer will not cancel the insured's coverage without giving thirty (30) calendar days prior written notice to the State.

[2] The State of California, its officers, agents, employees, and servants are included as additional insureds, but only with respect to work performed for the State under this Agreement and any extension or continuation of this Agreement.

[3] The insurance carrier shall notify CDPH, in writing, of the Contractor's failure to pay premiums; its cancellation of such policies; or any other substantial change, including, but not limited to, the status, coverage, or scope of the required insurance. Such notices shall contain a reference to each agreement number for which the insurance was obtained.

(f) The Contractor is hereby advised that copies of certificates of insurance may be subject to review and approval by the Department of General Services (DGS), Office of Risk and Insurance Management. The Contractor shall be notified by CDPH, in writing, if this provision is applicable to this Agreement. If DGS approval of the certificate of insurance is required, the Contractor agrees that no work or services shall be performed prior to obtaining said approval.

(g) In the event the Contractor fails to keep insurance coverage, as required herein, in effect at all times during vehicle possession, CDPH may, in addition to any other remedies it may have, terminate this Agreement upon the occurrence of such event.

3. Subcontract Requirements

(Applicable to agreements under which services are to be performed by subcontractors including independent consultants.)

a. Prior written authorization will be required before the Contractor enters into or is reimbursed for any subcontract for services exceeding $2,500 for any artices, supplies, equipment, or services. The Contractor shall obtain at least three competive quatations which should be submitted or adequate justification provided for the absence of bidding.

b. CDPH reserves the right to approve or disapprove the selection of subcontractors and with advance written notice, require the substitution of subcontractors and require the Contractor to terminate subcontracts entered into in support of this Agreement.

(1) Upon receipt of a written notice from CDPH requiring the substitution and/or termination of a subcontract, the Contractor shall take steps to ensure the completion of any work in progress and select a replacement, if applicable, within 30 calendar days, unless a longer period is agreed to by CDPH.

c. Actual subcontracts (i.e., written agreement between the Contractor and a subcontractor) exceeding $2,500 are subject to the prior review and written approval of CDPH.

d. Contractor shall maintain a copy of each subcontract entered into in support of this Agreement and shall, upon request by CDPH, make copies available for approval, inspection, or audit.

e. CDPH assumes no responsibility for the payment of subcontractors used in the performance of this Agreement. Contractor accepts sole responsibility for the payment of subcontractors used in the performance of this Agreement.

f. The Contractor is responsible for all performance requirements under this Agreement even though performance may be carried out through a subcontract.

g. The Contractor shall ensure that all subcontracts for services include provision(s) requiring compliance with applicable terms and conditions specified in this Agreement and shall be the subcontractor's sole point of contact for all matters related to the performance and payment during the term of this Agreement.

h. The Contractor agrees to include the following clause, relevant to record retention, in all subcontracts for services:

"(*Subcontractor Name*) agrees to maintain and preserve, until three years after termination of (*Agreement Number*) and final payment from CDPH to the Contractor, to permit CDPH or any duly authorized representative, to have access to, examine or audit any pertinent books, documents, papers and records related to this subcontract and to allow interviews of any employees who might reasonably have information related to such records."

4. Income Restrictions

Unless otherwise stipulated in this Agreement, the Contractor agrees that any refunds, rebates, credits, or other amounts (including any interest thereon) accruing to or received by the Contractor under this Agreement shall be paid by the Contractor to CDPH, to the extent that they are properly allocable to costs for which the Contractor has been reimbursed by CDPH under this Agreement.

5. Site Inspection

The State, through any authorized representatives, has the right at all reasonable times to inspect or otherwise evaluate the work performed or being performed hereunder including subcontract supported activities and the premises in which it is being performed. If any inspection or evaluation is made of the premises of the Contractor or Subcontractor, the Contractor shall provide and shall require Subcontractors to provide all reasonable facilities and assistance for the safety and convenience of the authorized representatives in the performance of their duties. All inspections and evaluations shall be performed in such a manner as will not unduly delay the services performed.

6. Intellectual Property Rights

a. Ownership

(1) Except where CDPH has agreed in a signed writing to accept a license, CDPH shall be and remain, without additional compensation, the sole owner of any and all rights, title and interest in all Intellectual Property, from the moment of creation, whether or not jointly conceived, that are made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement.

(2) For the purposes of this Agreement, Intellectual Property means recognized protectable rights and interest such as: patents, (whether or not issued) copyrights, trademarks, service marks, applications for any of the foregoing, inventions, trade secrets, trade dress, logos, insignia, color combinations, slogans, moral rights, right of publicity, author's rights, contract and licensing rights, works, mask works, industrial design rights, rights of priority, know how, design flows, methodologies, devices, business processes, developments, innovations, good will and all other legal rights protecting intangible proprietary information as may exist now and/or here after come into existence, and all renewals and extensions, regardless of whether those rights arise under the laws of the United States, or any other state, country or jurisdiction.

(a) For the purposes of the definition of Intellectual Property, "works" means all literary works, writings and printed matter including the medium by which they are recorded or reproduced, photographs, art work, pictorial and graphic representations and works of a similar nature, film, motion pictures, digital images, animation cells, and other audiovisual works including positives and negatives thereof, sound recordings, tapes, educational materials, interactive videos and any other materials or products created, produced, conceptualized and fixed in a tangible medium of expression. It includes preliminary and final products and any materials and information developed for the purposes of producing those final products. Works does not include articles submitted to peer review or reference journals or independent research projects.

(3) In the performance of this Agreement, Contractor will exercise and utilize certain of its Intellectual Property in existence prior to the effective date of this Agreement. In addition, under this Agreement, Contractor may access and utilize certain of CDPH's Intellectual Property in existence prior to the effective date of this Agreement. Except as otherwise set forth herein, Contractor shall not use any of CDPH's Intellectual Property now existing or hereafter existing for any purposes without the prior written permission of CDPH. **Except as otherwise set forth herein, neither the Contractor nor CDPH shall give any ownership interest in or rights to its Intellectual Property to the other Party.** If during the term of this Agreement, Contractor accesses any third-party Intellectual Property that is licensed to CDPH, Contractor agrees to abide by all license and confidentiality restrictions applicable to CDPH in the third-party's license agreement.

(4) Contractor agrees to cooperate with CDPH in establishing or maintaining CDPH's exclusive rights in the Intellectual Property, and in assuring CDPH's sole rights against third parties with respect to the Intellectual Property. If the Contractor enters into any agreements or subcontracts with other parties in order to perform this Agreement, Contractor shall require the terms of the Agreement(s) to include all Intellectual Property provisions. Such terms must include, but are not limited to, the subcontractor assigning and agreeing to assign to

CDPH all rights, title and interest in Intellectual Property made, conceived, derived from, or reduced to practice by the subcontractor, Contractor or CDPH and which result directly or indirectly from this Agreement or any subcontract.

(5) Contractor further agrees to assist and cooperate with CDPH in all reasonable respects, and execute all documents and, subject to reasonable availability, give testimony and take all further acts reasonably necessary to acquire, transfer, maintain, and enforce CDPH's Intellectual Property rights and interests.

b. Retained Rights / License Rights

(1) Except for Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement, Contractor shall retain title to all of its Intellectual Property to the extent such Intellectual Property is in existence prior to the effective date of this Agreement. Contractor hereby grants to CDPH, without additional compensation, a permanent, non-exclusive, royalty free, paid-up, worldwide, irrevocable, perpetual, non-terminable license to use, reproduce, manufacture, sell, offer to sell, import, export, modify, publicly and privately display/perform, distribute, and dispose Contractor's Intellectual Property with the right to sublicense through multiple layers, for any purpose whatsoever, to the extent it is incorporated in the Intellectual Property resulting from this Agreement, unless Contractor assigns all rights, title and interest in the Intellectual Property as set forth herein.

(2) Nothing in this provision shall restrict, limit, or otherwise prevent Contractor from using any ideas, concepts, know-how, methodology or techniques related to its performance under this Agreement, provided that Contractor's use does not infringe the patent, copyright, trademark rights, license or other Intellectual Property rights of CDPH or third party, or result in a breach or default of any provisions of this Exhibit or result in a breach of any provisions of law relating to confidentiality.

c. Copyright

(1) Contractor agrees that for purposes of copyright law, all works [as defined in Paragraph a, subparagraph (2)(a) of this provision] of authorship made by or on behalf of Contractor in connection with Contractor's performance of this Agreement shall be deemed "works made for hire". Contractor further agrees that the work of each person utilized by Contractor in connection with the performance of this Agreement will be a "work made for hire," whether that person is an employee of Contractor or that person has entered into an agreement with Contractor to perform the work. Contractor shall enter into a written agreement with any such person that: (i) all work performed for Contractor shall be deemed a "work made for hire" under the Copyright Act and (ii) that person shall assign all right, title, and interest to CDPH to any work product made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement.

(2) All materials, including, but not limited to, visual works or text, reproduced or distributed pursuant to this Agreement that include Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement, shall include CDPH's notice of copyright, which shall read in 3mm or larger typeface: "© *[Enter Current Year e.g., 2014, etc.]*, Department of Public Health. This material may not be reproduced or disseminated without prior written permission from the Department of Public Health." This notice should be placed prominently on the materials

and set apart from other matter on the page where it appears. Audio productions shall contain a similar audio notice of copyright.

d. Patent Rights

With respect to inventions made by Contractor in the performance of this Agreement, which did not result from research and development specifically included in the Agreement's scope of work, Contractor hereby grants to CDPH a license as described under Section b of this provision for devices or material incorporating, or made through the use of such inventions. If such inventions result from research and development work specifically included within the Agreement's scope of work, then Contractor agrees to assign to CDPH, without additional compensation, all its right, title and interest in and to such inventions and to assist CDPH in securing United States and foreign patents with respect thereto.

e. Third-Party Intellectual Property

Except as provided herein, Contractor agrees that its performance of this Agreement shall not be dependent upon or include any Intellectual Property of Contractor or third party without first: (i) obtaining CDPH's prior written approval; and (ii) granting to or obtaining for CDPH, without additional compensation, a license, as described in Section b of this provision, for any of Contractor's or third-party's Intellectual Property in existence prior to the effective date of this Agreement. If such a license upon the these terms is unattainable, and CDPH determines that the Intellectual Property should be included in or is required for Contractor's performance of this Agreement, Contractor shall obtain a license under terms acceptable to CDPH.

f. Warranties

(1) Contractor represents and warrants that:

(a) It is free to enter into and fully perform this Agreement.

(b) It has secured and will secure all rights and licenses necessary for its performance of this Agreement.

(c) Neither Contractor's performance of this Agreement, nor the exercise by either Party of the rights granted in this Agreement, nor any use, reproduction, manufacture, sale, offer to sell, import, export, modification, public and private display/performance, distribution, and disposition of the Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement will infringe upon or violate any Intellectual Property right, non-disclosure obligation, or other proprietary right or interest of any third-party or entity now existing under the laws of, or hereafter existing or issued by, any state, the United States, or any foreign country. There is currently no actual or threatened claim by any such third party based on an alleged violation of any such right by Contractor.

(d) Neither Contractor's performance nor any part of its performance will violate the right of privacy of, or constitute a libel or slander against any person or entity.

(e) It has secured and will secure all rights and licenses necessary for Intellectual Property including, but not limited to, consents, waivers or releases from all authors of music or performances used, and talent (radio, television and motion picture talent), owners of

any interest in and to real estate, sites, locations, property or props that may be used or shown.

(f) It has not granted and shall not grant to any person or entity any right that would or might derogate, encumber, or interfere with any of the rights granted to CDPH in this Agreement.

(g) It has appropriate systems and controls in place to ensure that state funds will not be used in the performance of this Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

(h) It has no knowledge of any outstanding claims, licenses or other charges, liens, or encumbrances of any kind or nature whatsoever that could affect in any way Contractor's performance of this Agreement.

(2) CDPH MAKES NO WARRANTY THAT THE INTELLECTUAL PROPERTY RESULTING FROM THIS AGREEMENT DOES NOT INFRINGE UPON ANY PATENT, TRADEMARK, COPYRIGHT OR THE LIKE, NOW EXISTING OR SUBSEQUENTLY ISSUED.

g. Intellectual Property Indemnity

(1) Contractor shall indemnify, defend and hold harmless CDPH and its licensees and assignees, and its officers, directors, employees, agents, representatives, successors, and users of its products, ("Indemnitees") from and against all claims, actions, damages, losses, liabilities (or actions or proceedings with respect to any thereof), whether or not rightful, arising from any and all actions or claims by any third party or expenses related thereto (including, but not limited to, all legal expenses, court costs, and attorney's fees incurred in investigating, preparing, serving as a witness in, or defending against, any such claim, action, or proceeding, commenced or threatened) to which any of the Indemnitees may be subject, whether or not Contractor is a party to any pending or threatened litigation, which arise out of or are related to (i) the incorrectness or breach of any of the representations, warranties, covenants or agreements of Contractor pertaining to Intellectual Property; or (ii) any Intellectual Property infringement, or any other type of actual or alleged infringement claim, arising out of CDPH's use, reproduction, manufacture, sale, offer to sell, distribution, import, export, modification, public and private performance/display, license, and disposition of the Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement. This indemnity obligation shall apply irrespective of whether the infringement claim is based on a patent, trademark or copyright registration that issued after the effective date of this Agreement. CDPH reserves the right to participate in and/or control, at Contractor's expense, any such infringement action brought against CDPH.

(2) Should any Intellectual Property licensed by the Contractor to CDPH under this Agreement become the subject of an Intellectual Property infringement claim, Contractor will exercise its authority reasonably and in good faith to preserve CDPH's right to use the licensed Intellectual Property in accordance with this Agreement at no expense to CDPH. CDPH shall have the right to monitor and appear through its own counsel (at Contractor's expense) in any such claim or action. In the defense or settlement of the claim, Contractor may obtain the right for CDPH to continue using the licensed Intellectual Property; or, replace or modify the licensed Intellectual Property so that the replaced or modified Intellectual Property becomes non-infringing provided that such replacement or modification is

functionally equivalent to the original licensed Intellectual Property. If such remedies are not reasonably available, CDPH shall be entitled to a refund of all monies paid under this Agreement, without restriction or limitation of any other rights and remedies available at law or in equity.

(3) Contractor agrees that damages alone would be inadequate to compensate CDPH for breach of any term of this Intellectual Property Exhibit by Contractor. Contractor acknowledges CDPH would suffer irreparable harm in the event of such breach and agrees CDPH shall be entitled to obtain equitable relief, including without limitation an injunction, from a court of competent jurisdiction, without restriction or limitation of any other rights and remedies available at law or in equity.

h. Survival

The provisions set forth herein shall survive any termination or expiration of this Agreement or any project schedule.

7. Prior Approval of Training Seminars, Workshops or Conferences

Contractor shall obtain prior CDPH approval of the location, costs, dates, agenda, instructors, instructional materials, and attendees at any reimbursable training seminar, workshop, or conference conducted pursuant to this Agreement and of any reimbursable publicity or educational materials to be made available for distribution. The Contractor shall acknowledge the support of the State whenever publicizing the work under this Agreement in any media. This provision does not apply to necessary staff meetings or training sessions held for the staff of the Contractor in order to conduct routine business matters.

8. Confidentiality of Information

The Contractor and its employees, agents, or subcontractors shall:

a. Protect from unauthorized disclosure names and other identifying information concerning persons either receiving services pursuant to this Agreement or persons whose names or identifying information become available or are disclosed to the Contractor, its employees, agents, or subcontractors as a result of services performed under this Agreement, except for statistical information not identifying any such person.

b. Not use such identifying information for any purpose other than carrying out the Contractor's obligations under this Agreement.

c. Promptly transmit to the CDPH Contract Manager all requests for disclosure of such identifying information not emanating from the client or person.

d. Not disclose, except as otherwise specifically permitted by this Agreement or authorized by the client, any such identifying information to anyone other than CDPH without prior written authorization from the CDPH Contract Manager, except if disclosure is required by State or Federal law.

e. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph.

f. As deemed applicable by CDPH, this provision may be supplemented by additional terms and conditions covering personal health information (PHI) or personal, sensitive, and/or confidential information (PSCI). Said terms and conditions will be outlined in one or more exhibits that will either be attached to this Agreement or incorporated into this Agreement by reference.

9. Documents, Publications and Written Reports

(Applicable to agreements over $5,000 under which publications, written reports and documents are developed or produced. Government Code Section 7550.)

Any document, publication or written report (excluding progress reports, financial reports and normal contractual communications) prepared as a requirement of this Agreement shall contain, in a separate section preceding the main body of the document, the number and dollar amounts of all contracts or agreements and subcontracts relating to the preparation of such document or report, if the total cost for work by nonemployees of the State exceeds $5,000.

10. Dispute Resolution Process

a. A Contractor grievance exists whenever there is a dispute arising from CDPH's action in the administration of an agreement. If there is a dispute or grievance between the Contractor and CDPH, the Contractor must seek resolution using the procedure outlined below.

(1) The Contractor should first informally discuss the problem with the CDPH Program Contract Manager. If the problem cannot be resolved informally, the Contractor shall direct its grievance together with any evidence, in writing, to the program Branch Chief. The grievance shall state the issues in dispute, the legal authority or other basis for the Contractor's position and the remedy sought. The Branch Chief shall render a decision within ten (10) working days after receipt of the written grievance from the Contractor. The Branch Chief shall respond in writing to the Contractor indicating the decision and reasons therefore. If the Contractor disagrees with the Branch Chief's decision, the Contractor may appeal to the second level.

(2) When appealing to the second level, the Contractor must prepare an appeal indicating the reasons for disagreement with Branch Chief's decision. The Contractor shall include with the appeal a copy of the Contractor's original statement of dispute along with any supporting evidence and a copy of the Branch Chief's decision. The appeal shall be addressed to the Deputy Director of the division in which the branch is organized within ten (10) working days from receipt of the Branch Chief's decision. The Deputy Director of the division in which the branch is organized or his/her designee shall meet with the Contractor to review the issues raised. A written decision signed by the Deputy Director of the division in which the branch is organized or his/her designee shall be directed to the Contractor within twenty (20) working days of receipt of the Contractor's second level appeal.

b. If the Contractor wishes to appeal the decision of the Deputy Director of the division in which the branch is organized or his/her designee, the Contractor shall follow the procedures set forth in Division 25.1 (commencing with Section 38050) of the Health and Safety Code and the

regulations adopted thereunder. (Title 1, Division 2, Chapter 2, Article 3 (commencing with Section 1140) of the California Code of Regulations).

c. Disputes arising out of an audit, examination of an agreement or other action not covered by subdivision (a) of Section 20204, of Chapter 2.1, Title 22, of the California Code of Regulations, and for which no procedures for appeal are provided in statute, regulation or the Agreement, shall be handled in accordance with the procedures identified in Sections 51016 through 51047, Title 22, California Code of Regulations.

d. Unless otherwise stipulated in writing by CDPH, all dispute, grievance and/or appeal correspondence shall be directed to the CDPH Contract Manager.

e. There are organizational differences within CDPH's funding programs and the management levels identified in this dispute resolution provision may not apply in every contractual situation. When a grievance is received and organizational differences exist, the Contractor shall be notified in writing by the CDPH Contract Manager of the level, name, and/or title of the appropriate management official that is responsible for issuing a decision at a given level.

11. Officials Not to Benefit

No members of or delegate of Congress or the State Legislature shall be admitted to any share or part of this Agreement, or to any benefit that may arise therefrom. This provision shall not be construed to extend to this Agreement if made with a corporation for its general benefits.

12. Prohibited Use of State Funds for Software

Contractor certifies that it has appropriate systems and controls in place to ensure that state funds will not be used in the performance of this Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

13. Contract Uniformity (Fringe Benefit Allowability)

(Applicable only to nonprofit organizations.)

Pursuant to the provisions of Article 7 (commencing with Section 100525) of Chapter 3 of Part 1 of Division 101 of the Health and Safety Code, CDPH sets forth the following policies, procedures, and guidelines regarding the reimbursement of fringe benefits.

a. As used herein fringe benefits shall mean an employment benefit given by one's employer to an employee in addition to one's regular or normal wages or salary.

b. As used herein, fringe benefits do not include:

(1) Compensation for personal services paid currently or accrued by the Contractor for services of employees rendered during the term of this Agreement, which is identified as regular or normal salaries and wages, annual leave, vacation, sick leave, holidays, jury duty and/or military leave/training.
(2) Director's and executive committee member's fees.
(3) Incentive awards and/or bonus incentive pay.
(4) Allowances for off-site pay.
(5) Location allowances.

(6) Hardship pay.
(7) Cost-of-living differentials

c. Specific allowable fringe benefits include:

(1) Fringe benefits in the form of employer contributions for the employer's portion of payroll taxes (i.e., FICA, SUI, SDI), employee health plans (i.e., health, dental and vision), unemployment insurance, worker's compensation insurance, and the employer's share of pension/retirement plans, provided they are granted in accordance with established written organization policies and meet all legal and Internal Revenue Service requirements.

d. To be an allowable fringe benefit, the cost must meet the following criteria:

(1) Be necessary and reasonable for the performance of the Agreement.
(2) Be determined in accordance with generally accepted accounting principles.
(3) Be consistent with policies that apply uniformly to all activities of the Contractor.

e. Contractor agrees that all fringe benefits shall be at actual cost.

f. Earned/Accrued Compensation

(1) Compensation for vacation, sick leave and holidays is limited to that amount earned/accrued within the agreement term. Unused vacation, sick leave and holidays earned from periods prior to the agreement term cannot be claimed as allowable costs. See section f (3)(a) below for an example.

(2) For multiple year agreements, vacation and sick leave compensation, which is earned/accrued but not paid, due to employee(s) not taking time off may be carried over and claimed within the overall term of the multiple years of the Agreement. Holidays cannot be carried over from one agreement year to the next. See Provision f (3)(b) for an example.

(3) For single year agreements, vacation, sick leave and holiday compensation that is earned/accrued but not paid, due to employee(s) not taking time off within the term of the Agreement, cannot be claimed as an allowable cost. See Provision f (3)(c) for an example.

(a) **Example No. 1:**

If an employee, John Doe, earns/accrues three weeks of vacation and twelve days of sick leave each year, then that is the maximum amount that may be claimed during a one year agreement. If John Doe has five weeks of vacation and eighteen days of sick leave at the beginning of an agreement, the Contractor during a one-year budget period may only claim up to three weeks of vacation and twelve days of sick leave as actually used by the employee. Amounts earned/accrued in periods prior to the beginning of the Agreement are not an allowable cost.

(b) **Example No. 2:**
If during a three-year (multiple year) agreement, John Doe does not use his three weeks of vacation in year one, or his three weeks in year two, but he does actually use nine weeks in year three; the Contractor would be allowed to claim all nine weeks paid for in year three. The total compensation over the three-year period cannot exceed 156 weeks (3 x 52 weeks).

(c) **Example No. 3:**
If during a single year agreement, John Doe works fifty weeks and used one week of vacation and one week of sick leave and all fifty-two weeks have been billed to CDPH, the remaining unused two weeks of vacation and seven days of sick leave may not be claimed as an allowable cost.

14. Cancellation

A. This agreement may be cancelled by CDPH **without cause** upon 30 calendar days advance written notice to the Contractor.

B. CDPH reserves the right to cancel or terminate this agreement immediately for cause. The Contractor may submit a written request to terminate this agreement only if CDPH substantially fails to perform its responsibilities as provided herein.

C. The term "for cause" shall mean that the Contractor fails to meet the terms, conditions, and/or responsibilities of this agreement.

D. Agreement termination or cancellation shall be effective as of the date indicated in CDPH's notification to the Contractor. The notice shall stipulate any final performance, invoicing or payment requirements.

E. Upon receipt of a notice of termination or cancellation, the Contractor shall take immediate steps to stop performance and to cancel or reduce subsequent agreement costs.

F. 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 cancellation and any non-cancelable obligations incurred in support of this agreement.

Exhibit E
Additional Provisions

1. Additional Incorporated Documents

A. The following documents and any subsequent updates are not attached, but are incorporated herein and made a part hereof by this reference. CDPH will maintain on file, all documents referenced herein and any subsequent updates, as required by program directives. CDPH shall provide the Contractor with copies of said documents and any periodic updates thereto, under separate cover.

1) Confidentiality Tables and Information Flows located at https://partners.cdph.ca.gov/sites/ADAPEnrollmentWorkers/

2) Quality Performance Metrics located at www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resourcespage.aspx

3) CDPH Guidelines located at https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_communications.aspx

4) AIDS Drug Assistance Program Formulary located at https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resourcespage.aspx

5) Pre-Exposure Prophylaxis Assistance Program Formulary located at https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OA_adap_resources_prepAP.aspx

6) AIDS Drug Assistance Program Enrollment Site Fee for Service Pay Schedule located at https://www.cdph.ca.gov/programs/cid/doa/pages/oa_adap_resourcespage.aspx

2. Insurance Requirements

A. General Provisions Applying to All Policies

1) Coverage Term – Coverage needs to be in force for the complete term of the Agreement. If insurance expires during the term of the Agreement, a new certificate and required endorsements must be received by the State at least ten (10) days prior to the expiration of this insurance. Any new insurance must comply with the original Agreement terms.

2) Policy Cancellation or Termination and Notice of Non-Renewal – Contractor shall provide to the CDPH within five (5) business days following receipt by Contractor a copy of any cancellation or non-renewal of insurance required by this Contract. In the event Contractor fails to keep in effect at all times the specified insurance coverage, the CDPH may, in addition to any other remedies it may have, terminate this Contract upon the occurrence of such event, subject to the provisions of this Contract.

3) Premiums, Assessments and Deductibles – Contractor is responsible for any premiums, policy assessments, deductibles or self-insured retentions contained within their insurance program.

4) Primary Clause – Any required insurance contained in this Agreement shall be primary and not excess or contributory to any other insurance carried by the CDPH.

5) Insurance Carrier Required Rating – All insurance companies must carry an AM Best rating of at least “A–” with a financial category rating of no lower than VI. If Contractor is

Exhibit E
Additional Provisions

self-insured for a portion or all of its insurance, review of financial information including a letter of credit may be required.

6) Endorsements – Any required endorsements requested by the CDPH must be physically attached to all requested certificates of insurance and not substituted by referring to such coverage on the certificate of insurance.

7) Inadequate Insurance – Inadequate or lack of insurance does not negate Contractor's obligations under the Agreement.

8) Use of Subcontractors - In the case of Contractor's utilization of Subcontractors to complete the contracted scope of work, Contractor shall include all Subcontractors as insured under Contractor's insurance or supply evidence of the Subcontractor's insurance to the CDPH equal to policies, coverages, and limits required of Contractor.

B. Insurance Coverage Requirements

Contractor shall display evidence of certificate of insurance evidencing the following coverage:

1) Commercial General Liability – Contractor shall maintain general liability with limits not less than $1,000,000 per occurrence for bodily injury and property damage combined with a $2,000,000 annual policy aggregate. The policy shall include coverage for liabilities arising out of premises, operations, independent Contractors, products, completed operations, personal and advertising injury, and liability assumed under an insured Agreement. This insurance shall apply separately to each insured against whom claim is made or suit is brought subject to Contractor's limit of liability. The policy shall be endorsed to include, "The State of California, its officers, agents, employees, and servants as additional insured, but only insofar as the operations under this Agreement are concerned." This endorsement must be supplied under form acceptable to the Office of Risk and Insurance Management.

2) Automobile Liability (when required) – Contractor shall maintain motor vehicle liability insurance with limits not less than $1,000,000 combined single limit per accident. Such insurance shall cover liability arising out of a motor vehicle including owned, hired and non-owned motor vehicles. Should the scope of the Agreement involve transportation of hazardous materials, evidence of an MCS-90 endorsement is required. The policy shall be endorsed to include, "The State of California, its officers, agents, employees, and servants as additional insured, but only insofar as the operations under this Agreement are concerned." This endorsement must be supplied under form acceptable to the Office of Risk and Insurance Management.

3) Worker's Compensation and Employer's Liability (when required) – Contractor shall maintain statutory worker's compensation and employer's liability coverage for all its employees who will be engaged in the performance of the Agreement. Employer's liability limits of $1,000,000 are required. When work is performed on State owned or controlled property the policy shall contain a waiver of subrogation endorsement in favor of the State. This endorsement must be supplied under form acceptable to the Office of Risk and Insurance Management.

4) Professional Liability (when required) – Contractor shall maintain professional liability covering any damages caused by a negligent error; act or omission with limits not less

Exhibit E
Additional Provisions

than $1,000,000 per occurrence and $1,000,000 policy aggregate. The policy's retroactive date must be displayed on the certificate of insurance and must be before the date this Agreement was executed or before the beginning of Agreement work.

5) Environmental/Pollution Liability (when required) – Contractor shall maintain pollution liability for limits not less than $1,000,000 per claim covering Contractor's liability for bodily injury, property damage and environmental damage resulting from pollution and related cleanup costs incurred arising out of the work or services to be performed under this Agreement. Coverage shall be provided for both work performed on site as well as transportation and proper disposal of hazardous materials. The policy shall be endorsed to include, "The State of California, its officers, agents, employees, and servants as additional insured, but only insofar as the operations under this Agreement are concerned." This endorsement must be supplied under form acceptable to the Office of Risk and Insurance Management.

6) Aircraft Liability (when required) - Contractor shall maintain aircraft liability with a limit not less than $3,000,000. The policy shall be endorsed to include, "The State of California, its officers, agents, employees and servants as additional insured, but only insofar as the operations under this Agreement." This endorsement must be supplied under form acceptable to the Office of Risk and Insurance Management.

Exhibit F
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.

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 CRF Parts 160 and 164.

H. Personal Information shall have the meaning given to such term in California Civil Code sections 1798.3 and 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 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.

Exhibit F
HIPAA Business Associate Addendum

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.

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.

e. 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.

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

   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 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,

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 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 1415 L Street, 5th Floor Sacramento, CA 95814 Email: privacy@cdph.ca.gov 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: cdphiso@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

Exhibit F
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':

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

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.

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 F
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 F
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.

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.

C. ***Confidential Destruction.*** CDPH PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

Exhibit F
HIPAA Business Associate Addendum

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.

MESSAGE FROM AIDS DRUG ASSISTANCE PROGRAM NOTICE OF PRIVACY PRACTICES

Effective May 30, 2019

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.

The 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. All information requested by ADAP must be provided in order participate in ADAP.

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, medical history, Social Security number, medical care given to you, and other personal information. 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 ADAP.
- **For 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 California State 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 disclose information ADAP has about you for the following reasons:

- To contact you about your ADAP benefits.
- 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.
- To Federal, State, or private entities for purposes of obtaining reimbursement for services as the payer of last resort; such activities may create an explanation of benefits that could be sent to a primary policyholder who may not be ADAP client.

ADAP may give out health information about you to organizations that help run ADAP. If ADAP does perform such disclosures, ADAP will protect the privacy of your information that ADAP shares.

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.
- 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 deny your access request, ADAP will give you information on how to appeal our decision.
- 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 to make a disclosure, or when ADAP shared your information 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 https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OAadap.aspx

HOW DO YOU CONTACT ADAP TO USE YOUR RIGHTS?

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

ADAP Health Insurance Portability and

Accountability Act Coordinator

c/o ADAP

Department of Public Health

MS 7704, P.O. Box 997426

Sacramento, CA 95899-7426

(844) 421-7050

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:

Privacy Officer

California Department of Public Health

Office of Legal Services

Privacy Office

1415 L Street

Suite 500

Sacramento, CA 95814

(877) 421-9634

privacy@cdph.ca.gov

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 7th Street, Suite 4-100, San Francisco, CA 94103, telephone (800) 368-1019, TDD (800) 537-7697, or email at ocrmail@hhs.gov.

ADAP cannot take away your health care benefits, 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 to this ADAP Notice of Privacy Practices. If ADAP does make any material changes, ADAP will amend this notice and give it to you right away.

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

State of California
Health and Human Services Agency

California Department of Public Health

MESSAGE FROM PrEP ASSISTANCE PROGRAM NOTICE OF PRIVACY PRACTICES

Effective June 18, 2019

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.

The Pre-Exposure Prophylaxis Assistance Program (PrEP-AP) must keep your health information private. PrEP-AP receives information about you when you apply for benefits and when your pharmacist sends PrEP-AP a bill for your care. PrEP-AP also receives medical information on your treatment when PrEP-AP approves your care. PrEP-AP must give you this notice about the law and how PrEP-AP can use and share your health information and what your rights are. All information requested by PrEP-AP must be provided in order participate in PrEP-AP.

HOW PrEP-AP MAY USE AND SHARE INFORMATION ABOUT YOU

PrEP-AP may only use and share information about you, as required or permitted by law, in the operation of PrEP-AP consistent with California Health and Safety Code section 120972. This information includes things like your name, address, medical history, Social Security number, medical care given to you and other personal information.

PrEP-AP uses this information and shares it with others for the following reasons:

- **For payment:** PrEP-AP and others that work with PrEP-AP review, approve, and pay for pharmacy bills sent to PrEP-AP for your medical care. When PrEP-AP does this, PrEP-AP shares information with the pharmacy benefits manager, pharmacists and doctors and others who bill PrEP-AP for your care.
- **For health care operations:** PrEP-AP 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 PrEP-AP drugs. PrEP-AP may also use this information in audits or fraud investigations, or for planning and managing PrEP-AP.
- **For eligibility determination:** PrEP-AP may share your PrEP-AP information with contractors for the purpose of PrEP-AP administration, including eligibility and enrollment activities.

PrEP-AP may also share your name and Social Security number or individual taxpayer identification number with the California State Franchise Tax Board. This allows PrEP-AP 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 PrEP-AP MAY SHARE YOUR INFORMATION

The law also allows PrEP-AP to use or disclose information PrEP-AP has about you for the following reasons:

- To contact you about your PrEP-AP benefits.
- When required by state or federal law.
- To agencies that oversee audits or investigations for purposes directly related to PrEP-AP.
- In appeals of decisions about health care claims paid or denied by PrEP-AP.
- To the federal government when it is checking on how PrEP-AP is meeting privacy laws.
- To other government agencies that give public benefits such as Medi-Cal, under specified conditions permitted by law.
- To Federal, State, or private entities for purposes of obtaining reimbursement for services as the payer of last resort; such activities may create an explanation of benefits that could be sent to a primary policyholder who may not be the PrEP-AP client.

PrEP-AP may give out health information about you to organizations that help run PrEP-AP. If PrEP-AP does perform such disclosures, PrEP-AP will protect the privacy of your information that PrEP-AP shares.

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. PrEP-AP will obey these laws.

WHEN WRITTEN PERMISSION IS NEEDED

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

IMPORTANT

PrEP-AP 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 PrEP-AP has shared your health information. The list will tell you what information PrEP-AP shared, with whom, when, and for what reasons. The list will not have when PrEP-AP gave information to you, when PrEP-AP had your permission to make a disclosure, or when PrEP-AP shared your information 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: https://www.cdph.ca.gov/Programs/CID/DOA/Pages/OAadap.aspx.

HOW DO YOU CONTACT PrEP-AP TO USE YOUR RIGHTS?

Please call or write PrEP-AP if you want to receive the form(s) you will need to exercise your privacy rights.

ADAP Health Insurance Portability and

Accountability Act Coordinator

c/o PrEP-AP

Department of Public Health

MS 7704, P.O. Box 997426

Sacramento, CA 95899-7426

(844) 421-7050

You may also contact your PrEP-AP enrollment worker for the forms necessary to exercise your rights.

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

Privacy Officer

California Department of Public Health

Office of Legal Services

Privacy Office

1415 L Street

Suite 500

Sacramento, CA 95814

(877) 421-9634

privacy@cdph.ca.gov

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 7th Street, Suite 4-100, San Francisco, CA 94103, telephone (800) 368-1019, TDD (800) 537-7697, or email at ocrmail@hhs.gov.

PrEP-AP cannot take away your health care benefits, 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

PrEP-AP must obey the rules of this notice. PrEP-AP has the right to make changes to this PrEP-AP Notice of Privacy Practices. If PrEP-AP does make any material changes, PrEP-AP will amend this notice and give it to you right away.

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

Exhibit I

Security Requirements, Protections, and Confidentiality Checklist

Enrollment Site Number:	**Enrollment Site Contact:**

Instructions:
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 CDPH/OA Enrollment Site meets, and shall continue to meet throughout the life of the contract, the requirements as identified in the Scope of Work exhibit 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.	☐

2a. Breaches of confidential client information must be <u>immediately</u> reported to CDPH/OA. In the space below, please identify the process and individual(s) your agency or organization has in place to report breaches of CDPH/OA clients' protected health or personal information. Attach additional page(s) if necessary.

_____

_____

_____

_____

3. The applicable Notices of Privacy Practices are posted in an area at the Enrollment Site that is accessible and visible to CDPH/OA applicants/clients.	☐

Please submit the completed Checklist to your CDPH/OA Advisor. All of the requirements listed above must be met in order to become an authorized Enrollment Site.

Exhibit I
Security Requirements, Protections, and Confidentiality Checklist

Enrollment Site Number:	**Enrollment Site Contact:**	
4. The Medication and Insurance Assistance Programs Grievance Form is posted in an area at the Enrollment Site that is accessible and visible to CDPH/OA applicants/clients		☐
5. The Contractor has internet access and scanning and uploading capabilities to allow for the creation of electronic client files within the designated CDPH/OA secure web-based enrollment system, AES.		☐
6. The Contractor has desktop computers, laptop computers, or other hand held electronic devices (shared or individual) with internet access available for all site personnel who will be performing CDPH/OA enrollment services.		☐
7. The Contractor fax machines, printers, scanners, and any other resource equipment used to transmit and/or receive CDPH/OA client enrollment information/documentation are located in a secure area at this Enrollment Site.		☐
8. The Contractor has ensured that all site personnel authorized to access the AES are trained in and use individual multi-factor authentication when connecting to the AES.		☐
Printed Name of Site Administrator	Signature of Site Administrator	Date Signed

Please submit the completed Checklist to your CDPH/OA Advisor. All of the requirements listed above must be met in order to become an authorized Enrollment Site.

Exhibit J
Plan for Transporting Confidential CDPH/OA Client Files

Enrollment Site Number:	**Enrollment Site Contact:**
Current Location (where client files are being transferred from): ES Address: _____ _____ _____ Date that Client Files will be Transferred/Transported: _____	**New Location** (where client files are being transferred to): ES Address: _____ _____ _____ ES Phone Number: ( )_____ ES Fax Number: ( )_____

Acknowledgement of CDPH/OA Policy for Transferring/Transporting Client Files:

It is the policy of CDPH/OA to ensure that any transfer of program or client documentation will be safe, secured, and implemented in accordance with CDPH/OA confidentiality and security requirements for safeguarding the confidentiality PHI). CDPH/OA EWs will implement and utilize reasonable and appropriate administrative, technical, and physical measures to safeguard PHI from any intentional or unintentional use or disclosure that might violate County, State, or Federal privacy regulations, Health and Safety Code or other applicable state legislation; and in accordance with the HIPAA BAA, and the Plan for Transporting Confidential CDPH/OA Client Files exhibits.

1. Why are client files being transferred?

☐ Relocation of the Enrollment Site to a new office/location
☐ Providing in-home client enrollment services when a client is unable to travel to the Enrollment Site
☐ Relocating client files to a new location for storage purposes
☐ Closure of Enrollment Site
☐ Other; enter below – you must contact your Advisor to discuss reasons not listed above:

_____

Please submit the completed Document Transfer Plan to your CDPH/OA Advisor. Your Advisor will contact you after the Document Transfer Plan has been reviewed/approved.

Exhibit J
Plan for Transporting Confidential CDPH/OA Client Files

Enrollment Site Number:	**Enrollment Site Contact:**
2. How many client files will be transferred? _____	
3. Describe the methods that will be used to secure client files when being transferred/transported (e.g., locked container, by vehicle/trunk, no stops on way to new location, etc.) _____ _____ _____ _____	
4. Which site staff person/s will supervise the security and transfer of client files as they are moved to the new location? Will a vendor be utilized? If so, please explain. _____ _____ _____ _____	

Please submit the completed Document Transfer Plan to your CDPH/OA Advisor. Your Advisor will contact you after the Document Transfer Plan has been reviewed/approved.

Exhibit J
Plan for Transporting Confidential CDPH/OA Client Files

Enrollment Site Number:	**Enrollment Site Contact:**
5. Describe where and how the client files will be stored at the new location. _____ _____ _____ _____	
6. Outline, step-by-step, the process that will be followed in the transferring of client files to the new location. Attach additional page(s) if necessary. _____ _____ _____ _____	
Printed Name and Title of Site Administrator	Signature of Site Administrator / Date Signed

Please submit the completed Document Transfer Plan to your CDPH/OA Advisor. Your Advisor will contact you after the Document Transfer Plan has been reviewed/approved.

Exhibit J
Plan for Transporting Confidential CDPH/OA Client Files

Additional Comments:

Please submit the completed Document Transfer Plan to your CDPH/OA Advisor. Your Advisor will contact you after the Document Transfer Plan has been reviewed/approved.

STATE OF CALIFORNIA

NONDISCRIMINATION CLAUSE *(OCP-1)*

STD. 17A (REV. 9-2000)

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, §12900 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.

Exhibit M
Restrictions and Requirements for the
Use and Disclosure of HIV/AIDS Public Health Data

This Attachment sets forth the HIV/AIDS-specific information use and disclosure requirements that Contractor is obligated to follow (in addition to all other confidentiality requirements set forth in the contract and other attachments thereto) with respect to all HIV/AIDS Public Health data disclosed to Contractor by the California Department of Public Health (CDPH).

I. Definitions: For purposes of this Agreement, the following definitions shall apply:

A. HIV/AIDS Public Health Data: "HIV/AIDS Public Health data" means confidential public health record or records collected or maintained by the CDPH Office of AIDS Programs, including but not limited to the AIDS Drug Assistance Program (ADAP), the Pre-Exposure Prophylaxis Assistance Program (PrEP-AP), and the HIV Care Program relating to human immunodeficiency virus (HIV) or acquired immunodeficiency syndrome (AIDS), containing personally identifying information, that were developed or acquired by a state public health agency, or an agent of that agency." Confidential public health record or records" is defined in Health and Safety (H&S) Code section 121035, subdivision (c), and means "any paper or electronic record maintained by the department or a local health department or agency, or its agent, that includes data or information in a manner that identifies personal information, including, but not limited to, name, social security number, address, employer, or other information that may directly or indirectly lead to the identification of the individual who is the subject of the record." HIV/AIDS Public Health data includes, but is not limited to: client name (first, middle initial, last), date of birth, and Social Security Number.

B. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information. "Disclosure" includes the disclosure, release, transfer, dissemination, or communication of all or any part of any confidential research record orally, in writing, or by electronic means to any person or entity, or providing the means for obtaining the records (H&S Code sections 121035 and 121125).

C. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of information.

II. Legal Authority for Disclosure and Use of HIV/AIDS Public Health Data: The legal authority for CDPH to collect, use, and disclose HIV/AIDS Public Health Data, and for Contractor to receive and use HIV/AIDS Public Health Data is as follows:

A. General Legal Authority:

1. Office of Aids (OA): H&S Code section 131019, provides as follows: "There is in the State Department of Public Health an Office of AIDS. The State Department of Public Health, Office of AIDS, shall be the lead agency within the state, responsible for coordinating state programs, services, and activities relating to the human immunodeficiency virus (HIV), acquired immune deficiency syndrome (AIDS), and AIDS related conditions (ARC)."

2. Office of Aids (OA): H&S Code section 131051, provides as follows: "The duties, powers, functions, jurisdiction, and responsibilities transferred to the State Department of Public Health shall, pursuant to the act that added this section, include all of the following previously performed by the former State Department of Health Services: (a) Under the jurisdiction of the Deputy Director for Prevention Services: (1) The Office of AIDS, including but not limited to: (A) The AIDS Drug Assistance Program (Chapter 6

Exhibit M
Restrictions and Requirements for the
Use and Disclosure of HIV/AIDS Public Health Data

(commencing with Section 120950) of Part 4 of Division 105).… (C) The CARE Services Program, provided for pursuant to the federal Ryan White CARE Act, 42 U.S.C. Section 300ff, (D) The CARE/Health Insurance Premium Payment Program (federal Ryan White CARE Act, 42 U.S.C. Sec. 300ff)…. (G) The AIDS Case Management Program (federal Ryan White CARE Act, 42 U.S.C. Sec. 300ff; Chapter 2 (commencing with Section 120815) of Part 4 of Division 105)."

B. AIDS Drug Assistance Program (ADAP) Legal Authority:

1. Legislative Intent for Drug Assistance: H&S Code section 120950, subdivision (b), provides as follows: "For reasons of compassion and cost effectiveness, the State of California has a compelling interest in ensuring that its citizens infected with the HIV virus have access to these drugs."

2. Subsidy for Drug Treatment: H&S Code section 120950, subdivision (c), provides as follows: "The department subsidizes the cost of these drugs for persons who do not have private health coverage, are not eligible for Medi-Cal, or cannot afford to purchase the drug privately. The subsidy program is funded through state and federal sources."

3. Establishment of ADAP: H&S Code section 120955, subdivision (a)(1), provides as follows: " To the extent that state and federal funds are appropriated in the annual Budget Act for these purposes, the director shall establish and may administer a program to provide drug treatments to persons infected with human immunodeficiency virus (HIV), the etiologic agent of acquired immunodeficiency syndrome (AIDS)."

4. Payer of Last Resort: H&S Code section 120955, subdivision (h), provides as follows: "Reimbursement under this chapter shall not be made for any drugs that are available to the recipient under any other private, state, or federal programs, or under any other contractual or legal entitlements, except that the director may authorize an exemption from this subdivision where exemption would represent a cost savings to the state."

5. Disclosure Permitted for ADAP Administration and Coordination of Client Eligibility: H&S Code section 120970, subdivision (i), provides as follows: "All types of information, whether written or oral, concerning a client, made or kept in connection with the administration of ADAP services, which includes subsidizing costs associated with health care service plan contracts and health insurance premium payment assistance, shall be confidential, and shall not be used or disclosed except … for purposes directly connected with the administration of the program," (paragraph 1); and "for coordinating client eligibility with programs funded by the federal Ryan White HIV/AIDS Program (Ryan White HIV/AIDS Treatment Extension Act of 2009, (Public Law 111-87, 42 U.S.C. Sec. 201, et seq.))" (paragraph 2).

C. Pre-Exposure Prophylaxis Assistance Program (PrEP-AP) Legal Authority:

1. General Authority: H&S Code section 120972, subdivision (a), provides as follows: "To the extent that funds are available for these purposes, the director may establish and administer a program within the department's Office of AIDS to subsidize certain costs of medications for the prevention of HIV infection and other related medical services, as authorized by this section…."

Exhibit M
Restrictions and Requirements for the
Use and Disclosure of HIV/AIDS Public Health Data

2. Disclosure Permitted for PrEP-AP Administration: H&S Code section 120972, subdivision (i), provides as follows: "All types of information, whether written or oral, concerning a client, made or maintained in connection with the administration of this program, shall be confidential, and shall not be used or disclosed except for any of the following: (1) For purposes directly connected with the administration of the program. (2) If disclosure is otherwise authorized by law."

D. California HIV/AIDS Disclosure Authority:

1. Disclosure Permitted for Public Health Purposes: H&S Code section 121025, subdivision (a), provides as follows: "Public health records relating to [HIV/AIDS], containing personally identifying information, that were developed or acquired by a state or local public health agency, or an agent of that agency, are confidential and shall not be disclosed, except as otherwise provided by law for public health purposes...."

2. Disclosure Permitted to Carry Out the Investigation, Control, or Surveillance Duties of CDPH and Contractor: H&S section 121025, subdivision (b), provides as follows: "In accordance with subdivision (g) of section 121022, a state or local public health agency, or an agent of that agency, may disclose personally identifying information in public health records... to other local, state, or federal public health agencies... when the confidential information is necessary to carry out the duties of the agency... in the investigation, control, or surveillance of disease, as determined by the state or local public health agency."

3. Only Minimum Necessary Disclosure Permitted: H&S Code section 121025, subdivision (c), provides as follows: "Any disclosures authorized... shall include only the information necessary for the purpose of that disclosure...."

4. Agreement Required: H&S Code section 121025, subdivision (c), provides as follows: "Except as provided in paragraphs (1) to (3), inclusive… any disclosure authorized by subdivision (a) or (b) shall not be made without written authorization as described in subdivision (a)...."

5. Disclosure for the Purpose of Facilitating Appropriate HIV/AIDS Medical Care and Treatment: H&S Code section 121025, subdivision (c)(2)(A), provides as follows: "State public health agency HIV surveillance staff, HIV prevention staff, AIDS Drug Assistance Program staff, and care services staff may further disclose the information to local public health agency staff, who may further disclose the information to the HIV-positive person who is the subject of the record, or the health care provider who provides his or her HIV care, for the purpose of proactively offering and coordinating care and treatment services to him or her."

6. State and Local Breach Investigation: H&S Code section 121022, subdivision (h), provides as follows: "(1) Any potential or actual breach of confidentiality of HIV-related public health records shall be investigated by the local health officer, in coordination with the department, when appropriate. The local health officer shall immediately report any evidence of an actual breach of confidentiality of HIV-related public health records at a city or county level to the department and the appropriate law enforcement agency. (2) The department shall investigate any potential or actual breach of confidentiality of HIV-

Exhibit M
Restrictions and Requirements for the
Use and Disclosure of HIV/AIDS Public Health Data

related public health records at the state level, and shall report any evidence of such a breach of confidentiality to an appropriate law enforcement agency."

III. Disclosure Restrictions: The Contractor and its employees or agents, shall protect from unauthorized disclosure any HIV/AIDS Public Health Data. The Contractor shall not disclose, except as otherwise specifically permitted by the contract between CDPH and Contractor, any HIV/AIDS Public Health Data to anyone other than CDPH, Office of AIDS, ADAP Branch, PrEP-AP, and HIV Care Branch staff. Contractor and its employees and agents shall not disclose any HIV/AIDS Public Health Data to persons who are not authorized by statute to receive such information, except if disclosure is required by state or federal law.

IV. Use Restrictions: The Contractor and its employees or agents, shall not use any HIV/AIDS Public Health Data for any purpose other than carrying out the Contractor's obligations under the contract between CDPH and Contractor (compare HIV/AIDS Public Health client data against Medi-Cal beneficiary data and provide results to CDPH), pursuant to the statutes and regulations set forth in Section II, above, or as otherwise allowed or required by state or federal law.

V. Confidentiality Agreements: All employees, agents, including subcontractors, to whom Contractor provides HIV/AIDS Public Health Data received from or created or received by Contractor, agree to the same restrictions and conditions that apply to Contractor with respect to such HIV/AIDS Public Health Data.

INFORMATION SECURITY OFFICE

Information Systems Security Requirements for Projects (ISO/SR1)

Version 4.0

February 2010

TABLE OF CONTENTS

I. PURPOSE **4**

II. SCOPE OF REQUIREMENTS **4**

III. CONTACT **4**

IV. INFORMATION SYSTEMS SECURITY REQUIREMENTS **5**

A. ADMINISTRATIVE / MANAGEMENT SAFEGUARDS 5
- *1. Workforce Confidentiality Statement* *5*
- *2. Access Authorization & Maintenance* *5*
- *3. Information System Activity Review* *5*
- *4. Periodic System Security & Log Review* *5*
- *5. Disaster Recovery Plan* *6*
- *6. Change Control* *6*
- *7. Supervision of Information* *6*
- *8. Escorting Visitors* *6*

B. TECHNICAL AND OPERATIONAL SAFEGUARDS 7
- *1. System Security Compliance* *7*
- *2. Malware Protection* *7*
- *3. Patch Management* *7*
- *4. Encrypted Electronic Transmissions* *7*
- *5. Encrypted Information Storage* *7*
- *6. Workstation / Laptop Encryption* *7*
- *7. Removable Media Encryption* *8*
- *8. Secure Connectivity* *8*
- *9. Intrusion Detection and Prevention* *8*
- *10. Minimum Information Download* *8*
- *11. Information Sanitization* *8*
- *12. Removal of Information* *8*
- *13. Faxing or Mailing of Information* *9*

C. SOLUTION ARCHITECTURE 10
- *1. System Security Compliance* *10*
- *2. Warning Banner* *10*
- *3. Layered Application Design* *10*
- *4. Input Validation* *11*
- *5. Data Queries* *11*
- *6. Username/Password Based Authentication* *12*
- *7. Administrative / Privileged Accounts Management* *12*
- *8. Service Accounts Management* *13*
- *9. Authentication and Authorization* *13*
- *10. Authentication Logging* *14*
- *11. Automatic System Session Expiration* *14*
- *12. Automatic System Lock-out and Reporting* *14*
- *13. Audit (Access)* *14*
- *14. Audit (Minimum Information)* *14*
- *15. Application Security Controls* *15*
- *16. Application Code Security* *15*
- *17. Strong Authentication* *16*

D. DOCUMENTATION OF SOLUTION 17
- *1. System Configuration* *17*
- *2. Information Classification* *17*
- *3. System Roles and Relationships* *17*
- *4. Audit Method Documentation* *17*
- *5. Retention of Documentation* *17*

E. ISO NOTIFICATIONS AND APPROVALS 18

1. Security Compliance Notification *18*
2. Notification of Changes to Solution *18*
3. Notification of Breach *18*
4. Project Security Approvals *18*
5. Application Security Approvals *19*
F. APPENDIX A – SR1 EXEMPTION FORM 20

Type: **ISO Requirements**	
Issued: **February 08, 2010**	*Doc Number:* **SR1 v4.0**
Revised:	
Title: **Information Systems Security Requirements for Projects**	

IMPORTANT NOTE: If an exemption from any SR1 requirement is required, the SR1 Exemption Form in Appendix A must be completed by the Project Manager or Contract Manager.

I. Purpose

This document provides the minimum security requirements mandated by the California Department of Public Health (CDPH) Information Security Office (ISO) for projects governed and/or subject to the policies and standards of CDPH. Projects that intend to deploy systems/applications into the CDPH system infrastructure, or will utilize CDPH information system services, are also subject to these minimum security requirements.

This document is intended to assist CDPH and its service customers in understanding the criteria CDPH will use when evaluating and certifying the system design, security features and protocols used by project solutions utilizing CDPH services. These security requirements will also be used in conjunction with the CDPH ISO compliance review program of its information system services customers.

This document will serve as a universal set of requirements which must be met regardless of physical hosting location or entities providing operations and maintenance responsibility. These requirements do not serve any specific project, nor do they prescribe any specific implementation technology.

II. Scope of Requirements

The information security requirements in this document are organized in five categories (sections) and address at a minimum:

- Administrative/Management Safeguards
- Technical and Operational Safeguards
- Solution Architecture
- Documentation of Solution
- ISO Notifications and Approvals

III. Contact

Chief Information Security Officer
California Department of Public Health
Information Security Office (ISO)
cdphiso@cdph.ca.gov

IV. Information Systems Security Requirements

A. Administrative / Management Safeguards

1. Workforce Confidentiality Statement

All persons working with CDPH information must sign a Security and Confidentiality Acknowledgement Statement. The Statement must include, at a minimum: General Use, Security and Privacy safeguards, Unacceptable Use, Audit and Enforcement policies. (Contact the CDPH ISO for the current version of the Security & Confidentiality Acknowledgement Statement in use.)

The Statement must be signed by the Project member prior to being granted access to the CDPH information. The Statement must be renewed annually.

2. Access Authorization & Maintenance

Project/Program must document and implement clearly defined rules and processes for vetting and granting authorizations, as well as procedures for the supervision of workforce members who work with CDPH information or in locations where it might be accessed.

On at least a semi-annual basis, Project/Program will review and remove all authorizations for individuals who have left the department, transferred to another unit, or assumed new job duties within CDPH.

3. Information System Activity Review

Project/Program must implement and document procedures to regularly review records of information system activity (such as audit logs, access reports, and security incident tracking reports).

Project/Program must ensure any hosting or maintenance agreements clearly identify responsibility for this activity. Logs may be stored within the system or preferably on a centralized logging server or service, and must be maintained for a minimum of three years.

4. Periodic System Security & Log Review

All systems must allow for periodic system security reviews that provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

These reviews may include technical tools and security procedures (such as vulnerability assessment products and penetration testing).

All systems processing and/or storing CDPH information must have a method or procedure in place to create and review system logs for unauthorized access. Logs may be stored within the system or on a centralized logging server or service, and must be maintained for a minimum of three years.

5. Disaster Recovery Plan

Project/Program will establish procedures that allow facility access in support of restoration of lost information under the Disaster Recovery Plan (DRP) and emergency mode operations plan in the event of an emergency.

The restoration/recovery support procedures must be added to the existing DRP to restore any loss of information and assure continuity of computing operations for support of both the application and information.

Recovery procedures must be developed using the most current DRP template provided by the CDPH ISO.

All systems, as part of a new or existing project, must allow for periodic system recovery testing. The period between tests should be defined as part of the project and be consistent with relevant CDPH disaster recovery standards. Such testing should provide assurances that plans and controls (management, operations, personnel, and technical) are functioning effectively and providing adequate levels of protection during an incident, disaster, or breach.

Project/Program will conduct an annual Business Impact Analysis of the application to determine the Maximum Acceptable Outage (MAO), cost of lost functionality, system component dependencies, business function dependencies, and business partner dependencies.

6. Change Control

All systems processing and/or storing CDPH information must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of information.

Systems running within the CDPH environment and/or utilizing CDPH services must comply with CDPH standards for change control process and procedures.

7. Supervision of Information

Classified information in paper form must 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. Classified information in paper form must also not be left unattended at any time in vehicles or planes, and must not be transported in checked-in baggage on commercial airplanes.

8. Escorting Visitors

Visitors to areas where classified information is contained must be escorted and classified information must be kept out of sight while visitors are in the area.

B. Technical and Operational Safeguards

1. System Security Compliance

All Project systems must comply with applicable CDPH security policies and requirements, as specified in the State Administrative Manual (SAM), Public Health Administrative Manual (PHAM), Privacy Act, and any other applicable State or Federal regulation. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

2. Malware Protection

All systems must install and actively use anti-virus software, with a minimum daily automatic update scheduled. Systems such as mainframes, where anti-virus is unavailable, are excluded from this requirement. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

3. Patch Management

All systems must install and actively use a comprehensive third-party patch management program, and routinely update system and application software within two weeks of vendor release unless the CDPH ISO validates a patch is not applicable. Critical updates may require a more restrictive timeline. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

4. Encrypted Electronic Transmissions

All information electronic transmissions that contain classified information (such as website access, file transfers or through e-mail) must be encrypted end-to-end using an industry-recognized encryption standard (such as Transport Layer Security (TLS) or its predecessor, Secure Socket Layer (SSL), Secure File Transfer Protocol (SFTP), or any FIPS 140-2 certified encryption algorithm). Classified information must be encrypted at the minimum of Advanced Encryption Standard (AES) with a 128 bit key or higher. Equivalent or stronger algorithms may be used upon approval of the CDPH ISO.

5. Encrypted Information Storage

All classified information must be encrypted when electronically stored using a CDPH approved encryption standard. Classified information must be encrypted at the minimum of AES with a 128 bit key or higher, or any FIPS 140-2 certified encryption algorithm. Equivalent or stronger algorithms may be used upon approval of the CDPH ISO.

6. Workstation / Laptop Encryption

All workstations and laptops that process and/or store classified CDPH information must be encrypted with a CDPH ISO approved solution. Classified CDPH information must be encrypted at the minimum of AES with a 128 bit key or higher, or any FIPS 140-2 certified encryption algorithm. Equivalent or stronger algorithms may be used upon approval of the CDPH ISO.

7. Removable Media Encryption

All electronic files that contain classified CDPH information must be encrypted at the minimum of AES with a 128 bit key or higher, or any FIPS 140-2 certified encryption algorithm when stored on any removable media type device (such as USB thumb drives, floppies, CD/DVD, tape backup, etc.). Equivalent or stronger algorithms may be used upon approval of the CDPH ISO. The solution should follow best practices described in National Institute of Standards & Technology (NIST) 800-111, Guide to Storage Encryption Technologies for End User Devices.

8. Secure Connectivity

All transmission and data-links between the information and application/system, and DBMS and the Office of Technology Services (OTech) Wide Area Network (WAN), must be secure between transmission systems as required by regulation, policy and/or standard and as prescribed for the given application/system.

9. Intrusion Detection and Prevention

All systems that are accessible via the Internet, are critical, and/or contain classified information must install and actively use a CDPH ISO approved comprehensive third-party real-time intrusion detection and prevention solution. The solution must also report security events directly to a CDPH enterprise monitoring solution. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

10. Minimum Information Download

In accordance with the principle of need-to-know, only the minimum amount of information required to perform necessary business functions should be copied or downloaded.

11. Information Sanitization

All classified CDPH information (electronic or paper) must be sanitized from systems when the information is no longer necessary. The sanitization method must conform to NIST Special Publication 800-88 Guidelines for Media Sanitization. Once information has been sanitized, the CDPH contract manager must be notified. If an agency or other entity is unable to sanitize the media in accordance with NIST 800-88 and provide notification, the media must be returned to CDPH after usage for sanitization in an approved manner.

12. Removal of Information

Classified CDPH information (electronic or paper) must not be removed from CDPH premises, or from the premises of an authorized vendor or contractor, without the written permission of the CDPH ISO.

13. Faxing or Mailing of Information

Facsimile transmissions containing classified CDPH information must not be left unattended if fax machines are not in a secure area. Facsimile transmissions must include a cover sheet that contains a security statement notifying persons receiving faxes in error to destroy them and notify the CDPH ISO immediately. Fax numbers must be verified before sending.

Classified CDPH information must only be mailed using secure methods. Large volume mailings of classified CDPH information must be by a secure, bonded courier with signature required upon receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH ISO approved solution.

C. Solution Architecture

1. System Security Compliance

The system must comply with all applicable CDPH security policies and requirements, as well as those specified in the State Administrative Manual (SAM), Public Health Administrative Manual (PHAM) Privacy Act, and any other applicable State or Federal regulation. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

The system may share data with other entities only after all applicable agreements are in place. For example, using a CDPH data release form, Business Associate Agreement, or Data Use Agreement. These agreements must ensure data is protected according to all applicable standards and policies.

Any data which is exported outside the scope of the system and its security provisions (such as exports for statistical analysis) require approval by the CDPH ISO to ensure sufficient security is in place to protect the exported data.

2. Warning Banner

All systems containing CDPH information must display a login warning banner stating that information is classified, activity is logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree and comply with these requirements.

The following warning banner must be used for all access points (such as desktops, laptops, web applications, mainframe applications, servers and network devices):

> ***WARNING: This is a State of California computer system that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.***
>
> ***LOG OFF IMMEDIATELY, if you do not agree to the conditions stated in this warning.***

3. Layered Application Design

Applications must be able to be segmented into a layered application design separating, at a minimum, the Presentation, Application/Business Logic, and Data Access Logic, and Data Persistence/Database layers.

The Presentation, Application/Business Logic, and Data Access Logic layers must be separated physically by a firewall regardless of physical implementation.

Any system request made to the Business logic layer must be authenticated.

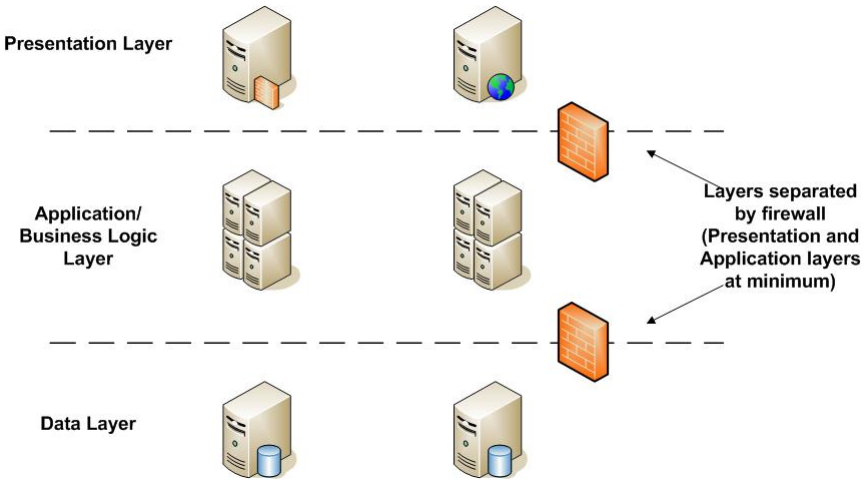
The Data Access Logic Layer may take the form of stored procedures, database Application Programming Interface (API), Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service. Any system request made to the Data Access

logic layer must be authenticated and authorized. No direct access to the Data Persistence/Database layer will be permitted, except through the Data Access logic layer.

All calls to the Data Persistence/Database layer will be made through the Data Access logic layer as a trusted sub-system that utilizes a single database access account to all transactions.

The Data Access Logic Layer must take the form of stored procedures, database API, Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service. System requests made to the Business logic and Data Access logic layers must be authenticated and authorized.

Vendor-provided commercial off-the-shelf (COTS) packages, or components where physical separation of layers is not possible, requires CDPH ISO approval.



4. Input Validation

All user input must be validated before being committed to the database or other application information repository. The system must manage client input controls from server side to the extent possible. Data queries from the Presentation or the Business Logic layers must be validated for appropriate use of query language, and validated for appropriate quantity and quality of data input. This includes In-line Structured Query Language (SQL) calls. The system must validate client input on the server side to the extent possible. All third-party client side input controls must be documented and approved by the CDPH ISO.

5. Data Queries

All Data queries (including In-line SQL calls) will not be allowed from the Presentation or the Business Logic layers unless validated for appropriate use of query language and validated for appropriate quantity/quality of data input. All data queries solution must be approved by the CDPH ISO.

Database table names and column names must not be exposed. Applications must use an alias for every table and column.

Dynamic SQL will not be permitted from the Presentation Layer without prior approval from the CDPH ISO.

6. Username/Password Based Authentication

When usernames and passwords are going to be used as the method for system authentication, the following requirements must be met:

- Username requirements:
  - Must be unique and traceable to an individual.
  - Must not be shared.
  - Must not be hard-coded into system logic.
- Password requirements:
  - Must not be shared.
  - Must be 8 characters or more in length.
  - Must not be a word found in the dictionary, regardless of language.
  - Must be encrypted using irreversible industry-accepted strong encryption.
  - Must be changed at least every 60 days.
  - Must not be the same as any of the previous 10 passwords.
  - Must be changed immediately if revealed or compromised.
  - Must be composed of characters from at least three of the following four groups from the standard keyboard:
    - Upper case letters (A-Z);
    - Lower case letters (a-z);
    - Numbers (0 through 9); and
    - Non-alphanumeric characters (punctuation symbols).
- Account security:
  - Accounts must be locked after three (3) failed logon attempts.
  - Account lock-out reset timers must be set for a minimum of 15 minutes.
  - Accounts must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password.

7. Administrative / Privileged Accounts Management

A privileged account is an account that allows an individual to perform maintenance on an operating system or applications (e.g. create/remove users, install applications, create/modify databases, etc.). Privileged accounts require the approval of the individual's manager, the CDPH ISO, and must include a business justification stating why privileged access is required and what it will be used for. Individuals granted privileged accounts must have already signed the Security and Confidentiality Acknowledgement Statement. (Contact the CDPH ISO for the current version of the Security & Confidentiality Acknowledgement Statement in use.)

The use of shared privileged accounts (e.g. Administrator) is strictly prohibited.

System administration must be performed using a different username rather than the one used for daily non-administrative activities. Administrative accounts must be used only for administrative activity within the authorized role of that account and the individual using it. It must be logged out of immediately after administrative work is complete.

- Username requirements:
  - Must be unique and traceable to an individual.
  - Must not be shared.
  - Must not be hard-coded into system logic.
  - Must be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
  - The default built-in Administrator account must be renamed and disabled.

    - The naming convention for privileged accounts must not make it obvious that usernames belong to privileged accounts.
    - If a generic privileged account is created:
        - Must only be used in an Emergency.
        - Must not be used for routine maintenance.
        - The password storage and management process for generic privileged accounts must be approved by the CDPH ISO.
- Password requirements:
    - Must not to be shared.
    - Must be 12 characters or more in length.
    - Must not be a word found in the dictionary, regardless of language.
    - Must be encrypted using irreversible industry-accepted strong encryption.
    - Must be changed at least every 60 days.
    - Must not be the same as any of the previous 10 passwords.
    - Must be changed immediately if revealed, or compromised.
    - Must be comprised 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);
        - Numbers (0 through 9);
        - Non-alphanumeric characters (punctuation symbols).
    - Must be changed immediately upon the termination or transfer of an employee with knowledge of the password.
    - Must not be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
- Account security:
    - Accounts must be locked after three (3) failed logon attempts.
    - Account lock-out timers must be set for at least 60 minutes.

8. Service Accounts Management

A service account is an account used to run a service and whose password is known by multiple individuals, When and where it is necessary to use a service account, the account request will be approved by the manager of the Project/Program requesting the account and by the CDPH ISO. Requirements, stating the need for a service account, will be documented in the request. A service account password is shared among the individuals authorized to access the account, and is subject to controls as stated in the password requirements in this document.

Restrictions for Service Accounts

- Sharing passwords via email is prohibited, unless the body of the email itself is encrypted using strong encryption.
- When users are no longer authorized to access an existing service account, the service account password must be changed.

9. Authentication and Authorization

Any system deployed during a project, or as a result of a project, must provide secure role-based access for authorization (separation between system/server administrators and application/database administrators) utilizing the principle of least privilege at all layers/tiers.

In all cases, applications must default to explicitly deny access where authentication and/or authorization mechanisms are required. No application that requires a login can offer to, or be capable of, remembering a user's credentials.

10. Authentication Logging

The system must log success and failures of user authentication at all layers as well as log all user transactions at the database layer as required by regulation, policy or standard, and as prescribed for the given application/system. This logging must be included for all user privilege levels including, but not limited to, systems administrators. This requirement applies to systems that process, store, and/or interface with CDPH information.

11. Automatic System Session Expiration

The system must provide an automatic timeout, requiring re-authentication of the user session after 20 minutes of inactivity.

12. Automatic System Lock-out and Reporting

The system must provide an automatic lock-out of users and a means to audit a minimum of three (3) failed log-in attempts. The means of providing audit information must be approved by the CDPH ISO.

13. Audit (Access)

All systems/applications will implement role-based access to auditing functions and audit trail information utilizing the principle of least privilege.

All systems/applications will implement a secure online interface to Audit Capabilities and Reporting by way of API or network service (or Web Service) to allow CDPH ISO to view logs, auditing procedures, and audit reporting.

14. Audit (Minimum Information)

The minimum log information below is required for any system that contains, or is involved in the transmission of, classified information. The log information should be available on every system running a production environment. This information must be provided upon request of the CDPH ISO for investigations and risk assessments.

The system must record, at minimum, the following events and any other events deemed appropriate by the CDPH ISO:

<u>Transaction Types</u>

- Any and all administrative changes to the system (such as administrative password changes, forgotten password resets, system variables, network configuration changes, disk sub-system modifications, etc).
- Logon failures.
- Logons during non-business hours.
- Failed access to an application or data.
- Addition, deletion, or modification of users or program access privileges.
- Changes in file access restrictions.
- Database addition, deletion, or modification.
- Copy of files before and after read/write changes.
- Transaction issued.

Individual audit trail records must contain the information needed to associate each query transaction to its initiator and relevant business purpose. Individual audit trail records should capture, at a minimum, the following:

Minimum Audit Trail Record Content

- Date and time stamp.
- Unique username of transaction initiator.
- Transaction recorded.
- Success or failure of transaction recorded.
- Relevant business process or application component involved.
- Data captured (if any).

Audit Trail logs must be maintained at minimum for three (3) years after the occurrence, or a set period of time determined by the CDPH ISO that would not hinder a detailed forensic investigation of the occurrence. The CDPH ISO has final approval authority.

15. Application Security Controls

For any application which accesses classified information, the following technical controls must be present, unless an exception is granted by the CDPH ISO:

- Must use *least privileged accounts* to execute code and to access databases.
- User access rights must be authenticated and authorized on entry to each application tier.
- All user input must be validated, including parameters passed to all public web service methods.
- Information that is not required must not be exposed.
- If a web application fails, it must not leave sensitive data unprotected or expose any details in error messages presented to the user. Any exceptions must be logged or emailed to the appropriate team member.
- Any sensitive data stored in session, cookies, disk files, etc., must be encrypted. Any sensitive data passed between tiers must be encrypted or must use SSL.
- Applications must be protected from the Internet by a front-end web application, firewall, gateway, and proxy of a type approved by the CDPH ISO, which must be included in the documented system design.
- Postback Universal Resource Locators (URLs) must not contain unencrypted record identifiers or database keys.
- Postback URLs must not include query strings.

16. Application Code Security

Application developers should use tools and methods during development to ensure all custom source code is free from security vulnerabilities. At a minimum, the application must be free of the vulnerabilities described in the CWE/SANS Top 25 Most Dangerous Programmer Errors (http://www.sans.org/top25errors/).

CDPH has the right to conduct a vulnerability scan against the application prior to its activation, and may disapprove use of the application until the vulnerabilities are remediated and the application re-tested. Any verified vulnerabilities from this list must be corrected by the organization which developed the application, at no additional cost to CDPH. Unless an exception is granted by the CDPH ISO, vulnerabilities identified within third-party components must be remediated by the third-party vendor at no additional cost to CDPH. Otherwise, a different third-party component must be selected and implemented.

17. Strong Authentication

Any information system providing access to Personally Identifiable Information (PII) and/or classified information from the Internet must assess the need for additional strong authentication, to prevent a significant data breach if a password is compromised. Strong authentication is defined as additional mandatory authentication over and beyond the password, for each account which has direct access to PII and/or classified information, or which has administrative privileges. The following factors should be included in the assessment:

- Applicable policies and regulations.
- Sensitivity of the PII or classified information.
- Number of data records.
- Number of user accounts with access to data.
- Level of control over end users.
- Level and frequency of log monitoring.
- Automated alerts and controls for unusual data access patterns.
- End user training on security practices.
- Other mitigating security controls.

The Project/Program providing access to PII and/or classified information from the Internet must either implement an approved strong authentication method, or document why strong authentication will not be utilized. This documentation must be provided to the CDPH ISO for review and approval.

The following methods are approved for strong authentication:

- **Physical Token:** A physical device in the possession of the account holder, which must be physically connected to the computer. Examples include a USB token or Smartcard.
- **One Time Password (OTP):** A temporary one time pass code is provided to the account holder, either by a physical device in their possession, or by way of a pre-defined communication channel such as cell phone or e-mail address. Examples include OTP token, or OTP sent via SMS text message, e-mail, or by automated voice call.
- **X.509 Certificate:** A digital certificate which has been installed on the access point computer or device, utilizing a Public Key Infrastructure (PKI).
- **Firewall Rules:** Firewall TCP/IP rules which ensure the account is only usable from an authorized access point, based upon specific IP address or IP subnet.

The following strong authentication method is approved for personal data access, where accounts have access to only the account holder's personal data, or a single data record they are custodian over such as a family member or information about their company. For example, an application where a client can submit or edit an enrollment form for themselves or someone else, but cannot access any other data records.

- **Personal Challenge Questions:** During registration, the account holder pre-answers one or more questions known only to them. When logging into a different computer, typically tracked with a cookie, they cannot login without correctly answering the pre-configured questions. The user should be prompted for whether the new computer is trusted vs. a one-time login, and this information used to determine whether to save a new cookie.

The proposed strong authentication mechanism must be included in the detailed design documentation as described in Section E.5, Application Security Approvals.

D. Documentation of Solution

1. System Configuration

Project/Program must document and maintain documentation for the system/application. This should include the following:

- Detailed design.
- Description of hardware, software, and network components.
- Special system configurations.
- External interfaces.
- All layers of security controls.

2. Information Classification

Project/Program will document and maintain an information classification matrix of all information elements accessed and/or processed by solution.

The matrix should identify at a minimum:

- Information element.
- Information classification/sensitivity.
- Relevant function/process, or where is it used.
- System and database, or where is it stored.

3. System Roles and Relationships

Project must document the following roles and ensure everyone understands their role, and complies with all applicable policies and regulations.

- The designated owner of the system.
- The designated custodian(s) of the system.
- The users of the system.
- The security administrator for the system.
- Outside entities sending or receiving data to system.

Project must document the organizational structure and relationships between these roles.

4. Audit Method Documentation

Project/Program will document the solution's auditing features and provide samples of audit reporting.

5. Retention of Documentation

The system/application administrators will retain documentation, including audit and activity logs, for a minimum of three (3) years (up to seven (7) years maximum) from the date of its creation or the date it was last in effect, whichever is later. Shorter retention periods must be allowed contingent upon applicable regulations, policies, and standards, and upon approval by the CDPH ISO. In certain circumstances the retention period must be lengthened to comply with regulatory requirements.

E. ISO Notifications and Approvals

1. Security Compliance Notification

As part of each project, assigned staff will document how the proposed solution meets or addresses the requirements specified in this document. This documentation must be submitted to the CDPH ISO prior to taking custody of CDPH information.

2. Notification of Changes to Solution

Once a project is approved as final by the CDPH ISO, no changes will be made to the project scope, documentation, systems or components without a change approval by the CDPH ISO.

3. Notification of Breach

The system/application administrators must immediately, and in writing, report to the CDPH ISO any and all breaches or compromises of system and/or information security. They must also take such remedial steps as may be necessary to restore security and repair damage, if any.

In the event of a breach or compromise of system and/or information security, the CDPH ISO may require a system/application security audit. The CDPH ISO must review the recommendations from the security audit, and make final decisions on the steps necessary to restore security and repair damage.

The system/application administrators must properly implement any and all recommendations of the security audit, as approved by the CDPH ISO.

4. Project Security Approvals

Projects must ensure checkpoints throughout the System Development Life Cycle (SDLC) which verify security requirements are being met. This must be incorporated in the project plan along with identification of necessary resources, timelines, and costs to address these requirements. The CDPH ISO should be involved throughout the SDLC to ensure this occurs.

For reportable Feasibility Study Reports (FSRs), the California Office of Information Security (OIS) requires submission of the *Questionnaire for Information Security and Privacy Components in Feasibility Study Reports and Project-Related Documents*.
See
http://www.cio.ca.gov/OIS/Government/documents/docs/Info_Sec_and_Priv_Components_FSR-Questionnaire.doc.

The response to this document must be approved by the CDPH ISO prior to submission.

Projects must ensure all applicable security requirements and deliverables are included in the project plan, and that ISO approvals are obtained, where required. This includes those listed in the following section, and any covered by other sections of this document. The CDPH ISO must be given reasonable time to review and comment on these deliverables.

5. Application Security Approvals

At a minimum, for any application which accesses classified information, the following documented CDPH ISO approvals must be obtained at the appropriate project phases, and before the application is moved to production.

- CDPH ISO approval of a dated, detailed design document. This design must include network layout including specific firewall port requirements, server hosting locations, operating systems, databases, data exchange interfaces, and points of authentication/authorization. The project must not move beyond the design phase until there is a CDPH ISO approved design.
- CDPH ISO approval of any non-standard development tools (such as programming languages or toolkits).
- CDPH ISO approval of a plan for an independent security code review which addresses at minimum the current Open Web Application Security Project (OWASP) top ten application vulnerabilities, and CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable. CDPH ISO must approve any findings of that code review not being corrected. CDPH ISO recommends the security code review be carried out during the development process rather than only at the end.
- CDPH ISO approval of a plan for security code reviews of future maintenance code changes, which addresses at minimum the current OWASP top ten application vulnerabilities, CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable.
- CDPH ISO approval of a plan for an independent automated security vulnerability assessment of the application, and approval of the findings of that assessment. The assessment must assess at minimum the OWASP top ten risks and CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable.

Independent as indicated above is defined as organizationally separate from those developing or configuration the application. The independence and skill level of the entities being utilized must be approved by the CDPH ISO.

Application code and infrastructure is subject to a CDPH ISO audit, and must match the approved detailed design.

F. Appendix A – SR1 Exemption Form

REF	Security Requirement	Exemption (Yes, No, or N/A)	Business Justification
A	**Administrative / Management Safeguards**		
1	Workforce Confidentiality Statement		
2	Access Authorization & Maintenance		
3	Information System Activity Review		
4	Periodic System Security & Log Review		
5	Disaster Recovery Plan		
6	Change Control		
7	Supervision of Information		
8	Escorting Visitors		
B	**Technical and Operational Safeguards**		
1	System Security Compliance		
2	Malware Protection		
3	Patch Management		
4	Encrypted Electronic Transmissions		
5	Encrypted Data Storage		
6	Workstation / Laptop Encryption		
7	Removable Media Encryption		
8	Secure Connectivity		
9	Intrusion Detection and Prevention		
10	Minimum Information Download		
11	Information Sanitization		
12	Removal of Information		
13	Faxing or Mailing of Information		
C	**Solution Architecture**		
1	System Security Compliance		
2	Warning Banner		
3	Layered Application Design		
4	Input Validation		
5	Data Queries		
6	Username/Password Based Authentication		
7	Administrative / Privileged Accounts Management		
8	Service Accounts Management		
9	Authentication and Authorization		
10	Authentication Logging		
11	Automatic System Session Expiration		
12	Automatic System Lock-out and Reporting		

REF	Security Requirement	Exemption (Yes, No, or N/A)	Business Justification
13	Audit (Access)		
14	Audit (Minimum Information)		
15	Application Security Controls		
16	Application Code Security		
17	Strong Authentication		
D	**Documentation of Solution**		
1	System Configuration		
2	Information Classification		
3	System Roles and Relationships		
4	Audit Method Documentation		
5	Retention of Documentation		
E	**ISO Notifications**		
1	Security Compliance Notification		
2	Notification of Changes to Solution		
3	Notification of Breach		
4	Project Security Approvals		
5	Application Security Approvals		

Exhibit O

Contractor's Release

Instructions to Contractor:

With final invoice(s) submit one (1) original and one (1) copy. The original must bear the original signature of a person authorized to bind the Contractor. The additional copy may bear photocopied signatures.

Submission of Final Invoice

Pursuant to **contract number** 20-10111 entered into between the California Department of Public Health (CDPH) and the Contractor (identified below), the Contractor does acknowledge that final payment has been requested via **invoice number(s)** _____, in the **amount(s) of $** _____ and **dated** _____.
If necessary, enter "See Attached" in the appropriate blocks and attach a list of invoice numbers, dollar amounts and invoice dates.

Release of all Obligations

By signing this form, and upon receipt of the amount specified in the invoice number(s) referenced above, the Contractor does hereby release and discharge the State, its officers, agents and employees of and from any and all liabilities, obligations, claims, and demands whatsoever arising from the above referenced contract.

Repayments Due to Audit Exceptions / Record Retention

By signing this form, Contractor acknowledges that expenses authorized for reimbursement does not guarantee final allowability of said expenses. Contractor agrees that the amount of any sustained audit exceptions resulting from any subsequent audit made after final payment will be refunded to the State.

All expense and accounting records related to the above referenced contract must be maintained for audit purposes for no less than three years beyond the date of final payment, unless a longer term is stated in said contract.

Recycled Product Use Certification

By signing this form, Contractor certifies under penalty of perjury that a minimum of 0% unless otherwise specified in writing of post consumer material, as defined in the Public Contract Code Section 12200, in products, materials, goods, or supplies offered or sold to the State regardless of whether it meets the requirements of Public Contract Code Section 12209. Contractor specifies that printer or duplication cartridges offered or sold to the State comply with the requirements of Section 12156(e).

Reminder to Return State Equipment/Property (If Applicable)

(Applies only if equipment was provided by CDPH or purchased with or reimbursed by contract funds)

Unless CDPH has approved the continued use and possession of State equipment (as defined in the above referenced contract) for use in connection with another CDPH agreement, Contractor agrees to promptly initiate arrangements to account for and return said equipment to CDPH, at CDPH's expense, if said equipment has not passed its useful life expectancy as defined in the above referenced contract.

Patents / Other Issues

By signing this form, Contractor further agrees, in connection with patent matters and with any claims that are not specifically released as set forth above, that it will comply with all of the provisions contained in the above referenced contract, including, but not limited to, those provisions relating to notification to the State and related to the defense or prosecution of litigation.

ONLY SIGN AND DATE THIS DOCUMENT WHEN ATTACHING IT TO THE FINAL INVOICE

Contractor's Legal Name (as on contract): County of Humboldt

Signature of Contractor or Official Designee: _____ Date: _____

Printed Name/Title of Person Signing: _____

Distribution: Accounting (Original) Program