Local Dental Pilot Project Application

Application Due Date: September 30, 2016

Revised July 28, 2016

General Instructions

Thank you for your interest in applying to participate in the Local Dental Pilot Project (LDPP) that is part of the State of California's Medi-Cal 2020 section 1115 waiver. In order to apply, the organization that is submitting the application must be one of the eligible entities as enumerated in the special terms and conditions (STCs) of the Medi-Cal 2020 section 1115 waiver, will designate a Lead Entity of the LDPP, and must complete and sign the entire application. Prior to completing this application, it is strongly suggested that applicants carefully review the STCs that govern the Medi-Cal 2020 section 1115 waiver, specifically the Dental Transformation Initiative (DTI), which is available on the Department of Health Care Services (DHCS) website at: http://www.dhcs.ca.gov/provgovpart/Pages/DTI.aspx. Other types of organizations not described in the special terms and conditions (STCs) may participate in the LDPP as a participating entity, as long as the organization has gained the sponsorship and is working with an approved applicant.

- Current Medi-Cal 2020 Special Terms and Conditions (STCs)
- *See STCs 104-109 and Attachment JJ for information relevant to the DTI.*

LDPP applicants may sponsor a single pilot project or multiple different pilot projects to test a variety of innovations aimed at meeting the goals of this domain. The goals of Domain 4 are to increase dental prevention; caries risk assessment and disease management, and continuity of care among Medi-Cal children through innovative pilot projects implemented by alternative programs, potentially using strategies focused on urban or rural areas, care models, delivery systems, workforce, integration of oral health into primary care, local case management initiatives and/or education. Progress toward reaching pilot project(s) goals and objectives will be measured, tracked and reported by selected LDPPs with the potential for regional and/or statewide expansion of pilot project(s) demonstrating a positive impact on the oral health of the targeted Medi-Cal child populations. The specific innovation that will be tested, strategies, target population(s), budget, payment methodologies, and participating entities shall be proposed by the entity submitting the application for participation. DHCS shall approve only those applications that meet the requirements to further the goals of one or more of the three following dental domains or other measures closely tied to the domains:

1. Increase preventive services utilization for children;
2. Increase caries risk assessment and disease management; and
3. Increase continuity of care

LDPPs are intended to target Medi-Cal child beneficiaries, ages twenty (20) and under, in need of dental services. LDPPs will identify the oral health needs of their targeted population and propose innovations, interventions and/or strategies that would be supported through the LDPP in their application. Applications will be expected to detail a pilot project's specific goals, anticipated outcomes, data that will be used to measure whether the project is having the intended impact, and the frequency of performance metric measurements. The goals, outcomes and performance metrics for analyzing the success of the pilot project should be consistent with and build upon the performance metrics of the DTI

Domains 1, 2 and 3 and should not be wholly redundant of the approaches taken in the aforementioned domains. LDPPs should consider the potential for statewide expansion, although some pilot projects may affect rural areas or only children in tribal communities.

Please complete the LDPP application and return it to DTI@DHCS.CA.GOV no later than 5:00 pm PT on September 30, 2016. Incomplete applications will not be considered. DHCS reserves the right to suspend or terminate an LDPP at any time if the enumerated goals are not met, corrective action has been imposed and not addressed, and/or poor performance continues despite corrective action.

In order for this application to be considered complete for purposes of submission, all components of the application must be completed, the application must be signed, and two attachments must be included:

1. (Required) Letters of Participation Agreements and/or Support for all participating entities.
2. (Required) A funding diagram illustrating how the requested funds would flow from DHCS to the Lead Entity and how the funds would be distributed among participating entities.
3. (Optional) A description of any requested requirement exceptions. For example: If a Lead Entity cannot reach agreement with a required participating entity.

Applications will be reviewed and selected based on the criteria and process outlined in **Appendix A**.

The application review process and timing is as follows:

Deliverable/Activity	Date
1. DHCS releases draft LDPP program Request for Applications (RFA) for public comment	May 13, 2016
2. DHCS conducts webinar to review LDPP application and respond to questions from potential applicants/interested entities	May 18, 2016
3. Public comments on LDPP application due to DHCS	May 20, 2016
4. DHCS releases final Revised LDPP RFA and selection criteria (Appendix A)	June 1, 2016
5. LDPP applications due to DHCS	September 30, 2016
6. DHCS completes application review and sends written questions/concerns to applicants	October 31, 2016
7. LDPP responds to DHCS questions/concerns	November 16, 2016
8. DHCS makes final decisions on approved LDPP applications	December 6, 2016
9. DHCS notifies CMS of final decisions on approved LDPP applications	December 6, 2016
10. DHCS notifies applicants of LDPP selection final decisions	December 6, 2016
11. Lead LDPP entity provides formal acceptance to DHCS	January 15, 2017
12. LDPP programs commence	February 15, 2017

Section 1: LDPP Lead Entity and Participating Entity Information

The purpose of this section is to provide information about the LDPP application and the designation of the Lead Entity and the other entities that will be participating in the LDPP.

Applicant Description

DHCS will accept applications for LDPPs from a county, a city and county, a consortium of counties serving a region consisting of more than one (1) county, a Tribe, an Indian Health Program, a University of California (UC) or California State University (CSU) campus.

Lead Entity Description

The LDPP Lead Entity, which must be a county/county entity[1], a city and county, a consortium of counties serving a region consisting of more than one (1) county, a Tribe, an Indian Health Program, a University of California (UC) or California State University (CSU) campus. Each LDPP application must

[1] DHCS is discussing with the federal Centers for Medicare and Medicaid Services regarding the use of a "county entity" as a Lead Entity for LDPPs. Updates on the outcome of the discussions will be posted in subsequent LDPP application FAQs.

designate the Lead Entity that will be responsible for coordinating the LDPP and be the single point of contact for DHCS and the Centers for Medicare and Medicaid Services (CMS). (STC 109.a)

Participating Entity Description

In addition to designating a Lead Entity, the LDPP application must identify other entities that will participate in the LDPP. Participating entities should represent a diverse set of key local community partners, educational entities, Medi-Cal providers, and stakeholders demonstrating community support and collaboration including Tribes and Indian health programs, with incentives related to goals and metrics of the overall proposal.

1.1 LDPP Lead Entity and Contact Person (STC 109.a)

Organization Name	
Type of Entity	☐ County ☐ County Entity[1] ☐ City and County ☐ Tribe ☐ Indian Health Program ☐ UC or CSU campus ☐ Consortium of counties serving a region consisting of more than one county
Contact Person	
Title	
Telephone	
Email Address	
Mailing Address	

1.2 Participating Entities

Identify the participating providers, entities and relevant stakeholders in the LDPP and clearly describe who they are, and explain their role in the LDPP. LDPP applicants may sponsor a single pilot project or multiple different pilot projects to test a variety of innovations aimed at meeting the goals of this domain. Please add additional rows as needed to the chart below.

Organization Name and Address	Description of Organization	Contact Name, Title, Telephone and Email	Role in LDPP
1.			
2.			
3.			
4.			
5.			
6.			

1.3 Letters of Participation/Support

As part of the application submission, attach letters of participation/support from participating providers, entities and other relevant stakeholders indicating their agreement to participate in and/or support the LDPP. Letters of participation/support should be on official letterhead and should clearly state its role with and/or support of the LDPP. (Attachment JJ.299.b.x)

1.4 Collaboration Plan

Describe a collaboration plan that includes participating entities and details how decisions will be made. Include information on how communication among the Lead Entity and the participating entities will occur, how silos will be minimized, and how issues will be resolved. (AttachmentJJ.299.b.ii)

Section 2: General Information and Target Population

The purpose of this section is to provide general information about the LDPP, the needs for the project and the target population.

LDPP Target Population Description

LDPP pilot projects must identify at-risk Medi-Cal children, up to age 20, who reside in the designated geographic area/region where the LDPP will operate and assess their unmet need to test innovations to increase prevention; caries risk assessment and disease management, and continuity of care. Pilot projects may focus on one or more target populations. Proposed interventions should not be wholly redundant of the DTI domains or duplicative of existing Medi-Cal services.

2.1 Target Population

The target population shall be identified through a needs assessment that was conducted to identify the target population(s), and include an estimated number of Medi-Cal beneficiaries to be served. The Lead Entity shall describe the needs assessment that was conducted and the data used. If the LDPP plans to have any enrollment caps for part or all of the pilot project(s), please provide information on the rationale for and level of the proposed cap for the target population(s). (AttachmentJJ.299.b.iii)

Section 3: Services, Interventions, Care Coordination and Data Sharing

The purpose of this section is to provide information about the pilot project(s) that will be implemented and tested under the LDPP. These unique innovations, interventions, and/or strategies may focus on urban or rural areas, care models, delivery systems, workforce, integration of oral health into primary care, local case management initiatives, education or other concepts that will be tested and evaluated for success. Applicants will describe how care may be coordinated and how data will be analyzed, shared and utilized by the participating entities. For purposes of reimbursement to participating providers, pilot projects cannot include payment for Medi-Cal covered services or expenditures that are directly reimbursed by the Medi-Cal Denti-Cal program for the target population in the geographic area(s) where the pilot project(s) is being implemented.

3.1 Services and Care Coordination

Describe the pilot project(s) that will operate under the LDPP. Describe the Medi-Cal Denti-Cal provider network that will deliver dental services. If applicable, describe how care coordination will be implemented including what each entity will be responsible for, and how the care coordination will be seamless to the beneficiary, taking into consideration other care coordination efforts by other pilot projects and/or other entities and how duplication of effort will be avoided. Examples of care coordination may include addressing appointment compliance barriers; coordination of oral health services across multiple providers, provider types, specialties, health care settings, health care organizations, and payment systems; motivational interviewing; and/or education to improve oral health literacy. For purposes of the LDPP, care coordination can be reimbursed using the funding awarded. If applicable, explain how pilot projects will work together to meet the goals envisioned under the DTI. (Attachment JJ.299.b.iv)

3.2 Innovations, Interventions, and Strategies

Describe the specific pilot project innovations, interventions and/or strategies that will be implemented and tested under the LDPP for the targeted population(s), including a quality improvement plan. Applications are expected to detail a pilot project's specific goals, anticipated outcomes, data that will be used to measure whether the project is having the intended impact, and the frequency of performance metric measurements. The goals, outcomes and performance metrics for analyzing the success of the pilot project should be consistent with and build upon the performance metrics of the three (3) DTI domains and should not be wholly redundant of the approaches taken in these domains. Applications should describe how the quality improvement plan will be incorporated to adjust, modify and learn from the pilot project activities implemented under the LDPP. (Attachment JJ.299.b.vi and b.viii)

3.3 Accountability

Describe how pilot projects will be monitored and the frequency of monitoring. Describe the quality improvement plan, how it will be used to adjust and modify pilot project activities and the frequency of quality improvement activities. Describe how the LDPP Lead Entity will assure compliance with its agreement with DHCS that specifies the requirements of the LDPP with STC109 and Attachment JJ of the Medi-Cal 2020 Waiver Special Terms and Conditions. Describe how the Lead Entity and participating entities will be accountable for ensuring that the targeted population receives timely, medically necessary care. (Attachment JJ.299.b.v)

3.4 Data Sharing

Describe how data sharing will occur between the LDPP and participating entities, including what data will be shared with whom and how data sharing will evolve over the life of the pilot. Indicate anticipated challenges and strategies the LDPP will employ to manage the challenges. (Attachment JJ.299.b.vii)

Section 4: Progress Reports and Ongoing Monitoring

The purpose of this section is to provide information on the progress reports the LDPP will use for ongoing monitoring of the participating entities performance.

Progress Reports Description

The LDPP shall submit quarterly and annual reports as agreed upon by DHCS and CMS upon approval of the LDPP. Continuation of the LDPP may be contingent on timely submission of all required reports.

4.1 LDPP Monitoring

Describe the Lead Entity's plan to conduct ongoing monitoring of the pilot projects and to make subsequent adjustments if poor performance or other issues are identified. This should include a process to provide technical assistance, impose corrective action and termination from the LDPP if poor performance is identified or continues. (AttachmentJJ.299.b.ix)

4.2 Data Analysis and Reporting

Describe the plan for ongoing data collection, analyses, and reporting of the LDPP innovations, interventions and/or strategies. Identify data that will be used to measure whether the project is having the intended impact, the source of the data, and the frequency of specific performance metric measurements and reporting. Describe how the data will be analyzed.

Section 5: Financing

Funding and Budget Description

Financing for up to 15 LDPPs is contingent upon the structure and design of approved applications and is limited to a maximum of twenty-five (25) percent of the annual funding limits – up to $185 million in total funds over the duration of the LDPP. The Department intends to begin this effort in a variety of select locations and subject to the demonstrated success of pilot project(s) and the availability of funding under the initiative, may seek to implement on a regional and/or statewide basis any pilot project(s) determined to be successful. The incentive funding available for preventive services, caries risk assessment and disease management, and continuity of care provided within this domain will not exceed the amount apportioned from the DTI pool for Domains 1, 2, and 3 for the applicable Demonstration Year. Incentive funding is payable only to enrolled Medi-Cal dental service locations.

5.1 Financing Structure

Describe the financing structure of the LDPP, including a description of how and to whom payments will be distributed. (Attachment JJ.299.b.xi)

5.2 Funding Request

Specify the total requested annual dollar amount for each of the Demonstration Years. Include the amounts for each element of funding that is proposed, including personnel costs, fringe benefits, operating expenses, equipment expenses, subcontractor expenses, travel expenses, other and indirect

costs. The funding request shall exclude covered services reimbursable by Medi-Cal Dental or other federal funding resources. The requested funding cannot supplant existing efforts that are currently being funded with Medi-Cal funds or locally funded projects for other sources. (AttachmentJJ.299.b.xi)

5.3 Budget
Provide the total annual requested budget amount and link it to expected value(s) or impact(s) that will be achieved each demonstration year (e.g., the performance of specific activities, interventions, supports and services, and/or outcomes) of the LDPP. (Attachment JJ.299.b.xii)

Section 6: Attestations and Certification

6.1 Attestation I certify that, as the representative of the LDPP Lead Entity, the Lead Entity agrees to the following conditions:

- ☐ The LDPP Lead Entity will assure appropriate participation in regular Learning Collaboratives to share best practices among participating entities, in accordance with STC 109.
- ☐ The LDPP Lead Entity will enter into an agreement with DHCS that specifies the requirements of the LDPP with STC109 and Attachment JJ of the Medi-Cal 2020 Waiver Special Terms and Conditions. The agreement with DHCS will include a data sharing agreement. See Exhibit A "HIPAA Business Associate Addendum (BAA)" of this Application. The provisions in the DHCS boilerplate BAA apply only to BAA-covered information that is shared by DHCS with the LDPP specifically for the purpose of LDPP operations and evaluation. DHCS does not anticipate that BAA-covered information will be shared for the purpose of LDPP operations or evaluation. DHCS anticipates limited, or no, BAA-covered information sharing from the LDPP to DHCS. However, DHCS will include a BAA in the event that data needs to be shared. The BAA will apply to the transfer of BAA-covered information should the need arise.
- ☐ The LDPP Lead Entity shall submit quarterly and annual reports in a manner specified by DHCS and CMS. Continuation of the LDPP may be contingent on timely submission of the quarterly and annual reports.
- ☐ The LDPP Lead Entity will report and submit timely and complete data to DHCS in a format specified by the State and as defined in the LDPP's individual agreement with the State. Incomplete and/or untimely data submissions may lead to a financial penalty after multiple occurrences and technical assistance is provided by the State.
- ☐ The LDPP Lead Entity will assure participation in program evaluation activities and will agree to provide data to measure the success of key activities of the work plan throughout the duration of the project.

I hereby certify that all information provided in this application is true and accurate to the best of my knowledge, and that this application has been completed based on a thorough understanding of program participation requirements as specified in the Medi-Cal 2020 Waiver Special Terms and Conditions and Attachment JJ of said waiver.

Signature of LDPP Lead Entity Representative **Date**

Appendix A: Application Selection Criteria

The Local Dental Pilot Project (LDPP) pilot application evaluation is a competitive process that will result in the selection of qualified LDPP pilots based on the quality and scope of their application. The application score will be factored into determining the funding amount for each LDPP pilot. The Department of Health Care Services (DHCS) will conduct the evaluation process in two phases: (1) Quality and Scope of Application and (2) Funding Decision. LDPP pilot applications that do not meet the basic requirements of the Special Terms and Conditions (STCs) and DHCS application guidance will be disqualified.

Overview

1) Quality and Scope of Application. LDPP pilot applications will be assigned a numerical score of up to 105 points based on the quality and scope of the application. ***Applications must achieve a minimum score of 77 points to be considered for participation in the LDPP pilot.*** Applications that achieve the minimum score and that include priority program elements will receive bonus points that may increase their possibility of participation. Applications must receive a pass score on all pass/fail criteria to be eligible to participate.

2) Funding Decision. The funding amount for each LDPP pilot will be determined based upon a combination of the funding request score and supporting financing information provided; comparisons to similarly-sized pilots based on specified county demographic and program design elements; and a final assessment of available funding relative to applications received.

Section 1: Quality and Scope of Application

A. Numerical Scores

Scoring criteria will help DHCS assess whether applications meet the LDPP pilot goals and requirements outlined in Medi-Cal 2020 Demonstration's STCs.

Each application will be assigned a numerical score based on a possible total of 105 points. Applicants must achieve a ***minimum score of 77 points*** to be considered to participate in the LDPP pilot. DHCS will use a reviewing panel to score applications and will assign an average total score to each application.

Highest Possible Score by Application Section	
Section	**Score**
Section 1: LDPP Lead Entity and Participating Entity Information	**10 points**
Section 2: General Information and Target Population	**20 points**
Section 3: Services, Interventions, Care Coordination, and Data Sharing	**35 points**
Section 4: Progress Reports and Ongoing Monitoring	**30 points**
Section 5: Financing	**10 points**
Section 6: Attestations and Certification	**Pass/Fail**
Total Possible Points	**105**

B. Scoring Criteria

Each application section will be scored based on the criteria specified below:

Section 1: LDPP Lead Entity and Participating Entity Information - 10 points

- ***1.1 Lead Entity Information: Pass/Fail***
  - Pass = Organization submitting the application meets lead entity requirements, and all required information is provided.
  - Fail = Lead entity does not meet lead entity requirements, and/or not all information is provided as required. The lead entity will be contacted and informed that they do not qualify as a lead entity.

- ***1.2 Participating Entities: 5 points***
  - Meets participating entity requirements as outlined in STC 109.
  - Information is complete.
  - Explanation of role in LDPP pilot is clear.
  - Has a diverse set of participating entities and key partners/stakeholders that are appropriate given the targeted population(s) and proposed strategies.
  - Fail = LDPP pilot does not meet the participating entity requirements or participating entities are not appropriate given the target population(s) and strategies.

- ***1.3 Letters of Participation/Support : Pass/Fail***
  - Pass = All letters provided.
  - Fail = Not all letters provided.

- ***1.4 Collaboration Plan: 5 points***
  - Describes a clear and comprehensive plan for collaboration, integration and communication between participating entities.
  - Describes mechanisms planned to minimize silos.

- Provides clear plan to communicate state pilot requirements from the lead entity to participating entities.
- Ability to provide learnings for potential future local efforts beyond the term of this demonstration.
- Describes how the pilot infrastructure and interventions may be sustained in absence of federal and state funding following the end of the pilot.
- Provides for a structure and process for decision making.
- Outlines a clear plan to convene regular meetings amongst the lead entity and participating providers/entities/relevant stakeholders.
- Identifies a main point of contact to support and coordinate with participating entities

Section 2: General Information and Target Population - 20 points

• 2.1 Target Population: 20 points

- Demonstrates community need for LDPP pilot.
- LDPP pilot design is comprehensive, cohesive, and well-designed to achieve goals.
- Demonstrates how the LDPP pilot will address community and target population needs.
- Scope is ambitious but realistic/achievable.
- Meets requirements outlined in STCs 106 - 108.
- Extent of scope and number of people in LDPP target population(s) and target population cap(s), if applicable.
- Target population(s) is/are appropriate given participating entities and strategies.
- Quality of methodology used to define target population(s).
- Provides a plan for beneficiary identification and outreach.

Section 3: Services, Interventions, Care Coordination and Data Sharing - 35 points

• 3.1 Services and Care Coordination: 10 points

- Provides a clear description of how care coordination will be implemented including what each participating entity will be responsible for, how community linkages with participating entities will occur and how such coordination will further the goals of the LDPP pilot project(s).
- Leverages and connects existing community infrastructure with the LDPP pilot project(s).
- Builds new infrastructure between lead and participating entities.

• 3.2 Innovations, Interventions, and Strategies: 10 points

- Meets requirements as outlined in the DTI STCs.
- Demonstrates appropriateness of services and interventions for target population(s).
- Describes a comprehensive approach of services, interventions, and strategies.
- Likelihood that interventions will be achievable and successful in improving dental health outcomes for target population(s).
- Alignment with other concurrent initiatives being implemented in the region (e.g., does the applicant articulate a vision of how pieces fit together).
- Describes infrastructure needed to implement the planned interventions taking into consideration what is feasible given timelines for implementation and ability to achieve planned goal(s) of the LDPP.
- Tests new innovations, interventions and strategies for the target population(s) and is not redundant of approaches taken in the three DTI domains.

• ***3.3 Accountability: 10 points***

- Describes project monitoring plan and frequency of monitoring.
- Clearly presents quality improvement plan and how project activities will be adjusted and modified to meet project goals.
- Details methods to ensure compliance with agreement with DHCS and requirements of STC 109 and Attachment JJ.
- Creates systems of accountability to assure targeted population receives timely, medically necessary care.

• ***3.4 Data Sharing: 5 points***

- Creates sustainable infrastructure to support data sharing between entities and identifies existing resources for data sharing and existing gaps.
- Increases care coordination across lead and participating entities.
- Clearly presents data sharing processes and expectations for what data is to be shared and means for protecting the data.
- Reasonableness and quality of timeline and implementation plan to develop necessary infrastructure.
- Quality of data governance structure and approach.

Section 4: Progress Reports and Ongoing Monitoring - 30 points

• ***4.1 LDPP Monitoring: 15 points***

- Identifies performance measures for each type of participating entity and the LDPP pilot itself, including short-term process measures and ongoing outcome measures; grouped by Demonstration Year, including an annual target benchmark.
- Demonstrates comprehensive plan for collecting, tracking, and documenting metrics.
- Quality of plan to conduct ongoing monitoring and make adjustments as needed.
- Comprehensive plan for providing technical assistance, imposing corrective action, and terminating if poor performance is identified and continues.

• ***4.2 Data Analysis and Reporting: 15 points***

- Describes a clear and high-quality plan for ongoing data collection, reporting, and analysis of interventions and strategies.
- Describes a clear plan for using analysis for sustainability planning.

Section 5: Financing - 10 points (7 point minimum required score)

- Demonstrates reasonableness of the amount of the funding request in relation to proposed LDPP pilot activities
- Provides detail of the total funding amount requested, by Demonstration Years for each deliverable requested, including baseline data collection, infrastructure, interventions, and outcomes.
- Describes a comprehensive approach how to flow funds, how reimbursement will take place and oversight and monitoring of payment.
- Provides reasonable methodology for establishing the budget request.
- Clear description or diagram explaining how the payment process will function.

- Alignment with/leverage of other funding sources.

Section 6: Attestations and Certification-Pass/Fail

- Pass = Applicant checks box and provides signature.
- Fail = Applicant does not check box and/or does not include a signature. Applicant may not participate in a LDPP pilot unless Section 6 receives a score of "Pass."

Bonus Points: Awarded to Applications That Include Priority Elements

LDPP pilot applications may qualify to receive bonus points if they include certain priority program elements in their LDPP pilot. Applicants must achieve a minimum numerical score of 77 points (NOT including bonus points) in order to participate in the LDPP pilot. These LDPP pilots may then qualify for bonus points.

Priority Elements That Receive Bonus Points:

- **Collaboration:** At least one participating Tribe, Indian Health Program, UC or CSU campus in the geographic areas where the pilot operates (**maximum of 5 points**).
- **Community partners:** More than two participating key community partners in the geographic areas where the pilot operates (**maximum of 5 points**).
- **Interventions:** Innovative interventions (**maximum of 5 points**)
  - Creative interventions, such as creative workforce strategies (e.g., effective use of community health workers); appropriately targeting digital health tools or other health information technology solutions; and engaging extensively with community partners.
  - Creative financing/use of innovative incentive payment models that will help inform the use of value-based purchasing in the future.

Section 2: Funding Decision

A. Funding Allocation Will Be Determined Based on Three Factors

Funding will be determined based on the funding request and application financing responses, comparisons to similarly-sized pilots, and an assessment of available funds relative to applications received.

<u>Funding Decision Criteria</u>

1) **Funding request and quality of financing application responses.**
   The funding request and the financing application responses will be assessed and scored according to the Application Section 5 "Financing" scoring criteria listed above, including the annual budget amount requested for each individual item for which funding is requested, including baseline data collection, infrastructure, interventions, and outcomes. DHCS will determine the appropriateness of the funding request given the scope and ambitiousness of the pilot, how well the applicant demonstrates the soundness of their approach, the clarity of the governance structure, presence of oversight mechanisms and internal controls to ensure payment and accountability related to

participating entities, the needs of the target population, the complexity of the interventions, and ensure that payments are not duplicative of payments for existing services.

2) **Comparisons to similarly-sized pilots.**
Funding requests from similarly-sized LDPP applications will be compared based on pilot scope, design, and funding requested.

3) **Assessment of Available Funding.**
DHCS will assess the availability of funds relative to the applications received. If assigned funding amounts exceed the maximum available, either funding amounts for approved pilots will be reduced to meet the funding limitations or some pilots will not be approved.

Exhibit A
HIPAA Business Associate Addendum

I. Recitals

A. This Contract (Agreement) 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 Health Care Services ("DHCS") wishes to disclose to Business Associate certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.

C. As set forth in this Agreement, Contractor, here and after, is the Business Associate of DHCS acting on DHCS' behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of DHCS and creates, receives, maintains, transmits, uses or discloses PHI and PI. DHCS and Business Associate are each a party to this 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 this 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 DHCS 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, and the Final Omnibus Rule as well as the Alcohol and Drug Abuse patient records confidentiality law 42 CFR Part 2, and any other applicable state or federal law or regulation. 42 CFR section 2.1(b)(2)(B) allows for the disclosure of such records to qualified personnel for the purpose of conducting management or financial audits, or program evaluation. 42 CFR Section 2.53(d) provides that patient identifying information disclosed under this section may be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by an appropriate court order.

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, the HIPAA regulations, and the Final Omnibus Rule.

B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the final Omnibus Rule.

C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and Final Omnibus Rule.

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 CFR Parts 160 and 164.

H. Personal Information shall have the meaning given to such term in California Civil Code section 1798.29.

I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.

J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an

authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.

L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.

M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.

N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act, and the HIPAA regulations.

III. Terms of Agreement

A. Permitted Uses and Disclosures of PHI by Business Associate

Permitted Uses and Disclosures. Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of DHCS, provided that such use or disclosure would not violate the HIPAA regulations, if done by DHCS. 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, the HIPAA regulations, the Final Omnibus Rule and 42 CFR Part 2.

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 DHCS. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of DHCS with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of DHCS.

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 DHCS 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 this 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 DHCS, 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 this 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 DHCS 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 DHCS under this 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 this Agreement.

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

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 DHCS, 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 the HIPAA regulations, and the Final Omnibus Rule, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI and PI. Business associates are directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. Business Associate shall incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PI be reported to Business Associate.

2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:

    a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by DHCS; 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 DHCS and Individuals.*** To provide access and information:

1. To provide access as DHCS may require, and in the time and manner designated by DHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to DHCS (or, as directed by DHCS), to an Individual, in accordance

with 45 CFR section 164.524. Designated Record Set means the group of records maintained for DHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DHCS health plans; or those records used to make decisions about individuals on behalf of DHCS. Business Associate shall use the forms and processes developed by DHCS for this purpose and shall respond to requests for access to records transmitted by DHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

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 DHCS 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 DHCS that was provided to DHCS by the Social Security Administration, upon request by DHCS, Business Associate shall provide DHCS 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 DHCS directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner designated by DHCS.

H. ***Internal Practices.*** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from DHCS, or created or received by Business Associate on behalf of DHCS, available to DHCS or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by DHCS or by the Secretary, for purposes of determining DHCS' 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 DHCS and shall set forth the efforts it made to obtain the information.

I. ***Documentation of Disclosures***. To document and make available to DHCS or (at the direction of DHCS) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with 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 DHCS 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 DHCS 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 this 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 DHCS*.** (1) To notify DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to DHCS by the Social Security Administration. This notification will be **by telephone call plus email or fax** upon the discovery of the breach. (2) To notify DHCS **within 24 hours by email or fax** of the discovery 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, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this 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 DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to DHCS by the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS 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 DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link:

http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

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. If the initial report did not include all of the requested information marked with an asterisk, then within 72 hours of the discovery, Business Associate shall submit an updated "DHCS 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 DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer:

3. ***Complete Report***. To provide a complete report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. If all of the required information was not included in either the initial report, or the Investigation Report, then a separate Complete Report must be submitted. The report shall be submitted on the "DHCS 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 DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide DHCS 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 "DHCS Privacy Incident Report" form. DHCS will review and approve or disapprove the determination of whether a breach occurred, is

reportable to the appropriate entities, if 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 DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS 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 DHCS in addition to Business Associate, Business Associate shall notify DHCS, and DHCS 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. ***DHCS Contact Information.*** To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated herein. DHCS reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

DHCS Program Contract Manager	**DHCS Privacy Officer**	**DHCS Information Security Officer**
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Fax: (916) 440-5537 Telephone: EITS Service Desk (916) 440-7000 or (800) 579-0874

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 DHCS of this Addendum, it shall take the following steps:

1. Provide an opportunity for DHCS to cure the breach or end the violation and terminate the Agreement if DHCS does not cure the breach or end the violation within the time specified by Business Associate; or
2. Immediately terminate the Agreement if DHCS 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 DHCS

DHCS agrees to:

A. ***Notice of Privacy Practices***. Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR section 164.520, as well as any changes to such notice. Visit the DHCS Privacy Office to view the most current Notice of Privacy Practices at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx or the DHCS website at www.dhcs.ca.gov (select "Privacy in the left column and "Notice of Privacy Practices" on the right side of the page).

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

C. ***Notification of Restrictions***. Notify the Business Associate of any restriction to the use or disclosure of PHI that DHCS has agreed to in accordance with 45 CFR 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 DHCS.

V. Audits, Inspection and Enforcement

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

1. Failure to detect or

2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitutes acceptance of such practice or a waiver of DHCS' enforcement rights under this 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 DHCS and provide DHCS 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 contract and shall terminate when all the PHI provided by DHCS to Business Associate, or created or received by Business Associate on behalf of DHCS, is destroyed or returned to DHCS, 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 DHCS' knowledge of a material breach or violation of this Addendum by Business Associate, DHCS shall:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by DHCS; or

2. Immediately terminate this 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 DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. DHCS may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. DHCS may terminate this Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.

D. ***Effect of Termination.*** Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from DHCS (or created or received by Business Associate on behalf of DHCS) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify DHCS of the conditions that make the return or destruction infeasible, and DHCS 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.*** DHCS makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

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

HITECH Act, the HIPAA regulations or other applicable laws. DHCS may terminate this Agreement upon thirty (30) days written notice in the event:

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

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

C. ***Assistance in Litigation or Administrative Proceedings***. Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, 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 DHCS or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

E. ***Interpretation***. The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the 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 this Agreement.

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

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 DHCS, or access or disclose DHCS 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 DHCS 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 DHCS PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.

D. ***Background Check.*** Before a member of the workforce may access DHCS 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 DHCS 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 DHCS Information Security Office.

B. ***Server Security.*** Servers containing unencrypted DHCS 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 DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

D. ***Removable media devices.*** All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

E. ***Antivirus software.*** All workstations, laptops, and other systems that process and/or store DHCS 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 DHCS 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 DHCS 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 DHCS PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.

I. ***System Timeout.*** The system providing access to DHCS 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 DHCS 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 DHCS PHI or PI, or which alters DHCS 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 DHCS 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 DHCS 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 DHCS 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 DHCS 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 DHCS 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 DHCS 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 DHCS 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 DHCS 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 this Agreement for more than 24 hours.

B. ***Data Backup Plan.*** Contractor must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS 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 DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

V. Paper Document Controls

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

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

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

E. ***Faxing.*** Faxes containing DHCS 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 DHCS 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 DHCS 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 DHCS to use another method is obtained.

UC HIPAA Business Associate Addendum

I. Recitals

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

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

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

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

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

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

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

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

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

1. Permitted Uses and Disclosures of PHI by Business Associate

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

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

1) ***Use and disclose for management and administration.*** Use and disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

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

2. Responsibilities of Business Associate

Business Associate agrees:

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

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

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

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

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

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

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

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

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

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

F. ***Availability of Information to DHCS and Individuals.*** If Business Associate creates or maintains the Designated Record Set on behalf of DHCS, Business Associate will provide access as DHCS may require, and in the time and manner designated by DHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to DHCS (or, as

directed by DHCS), to an Individual, in accordance with 45 CFR Section 164.524. Designated Record Set means the group of records maintained by Business Associate for DHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DHCS health plans; or those records used to make decisions about individuals on behalf of DHCS. Business Associate shall use the forms and processes developed and provided by DHCS for this purpose and shall respond to requests for access to records transmitted by DHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

K. ***Workforce Training and Discipline***. To train and use reasonable measures to provide for compliance with the requirements of this Addendum by workforce members who assist in the performance of functions or activities on behalf of DHCS under this Agreement and use or disclose PHI; and discipline such workforce members who intentionally violate any provisions of this Addendum, with possible sanctions to include termination of employment. In complying with the provisions of this section, Business Associate shall observe the following requirements:

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

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

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

3. Obligations of DHCS

DHCS agrees to:

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

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

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

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

4. Audits, Inspection and Enforcement

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

A. Failure to detect or

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

5. Termination

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

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

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

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

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

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

6. Miscellaneous Provisions

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

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

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

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

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

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

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

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

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

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

Attachment A
Business Associate Data Security Requirements

A. General Security Controls

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

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

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

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

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

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

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

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

i. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DHCS data. Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed

every 60 days. Must be changed if revealed or compromised. Must be composed of characters from at least three of the following four groups from the standard keyboard:

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

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

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

B. System Security Controls

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

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

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

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

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

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

C. Audit Controls

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

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

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

D. Business Continuity / Disaster Recovery Controls

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

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

E. Paper Document Controls

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

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

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

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

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

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