

Contractor's Release

Instructions to Contractor:

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

Submission of Final Invoice

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

Release of all Obligations

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

Repayments Due to Audit Exceptions / Record Retention

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

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

Recycled Product Use Certification

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

Reminder to Return State Equipment/Property (If Applicable)

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

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

Patents / Other Issues

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

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

Contractor's Legal Name (as on contract): _____

Signature of Contractor or Official Designee: _____ Date: _____

Printed Name/Title of Person Signing: _____

Distribution: Accounting (Original) Program

Travel Reimbursement Information
(Lodging and Per Diem Reimbursement Increase – Effective for travel on/after January 1, 2015)

1. The following rate policy is to be applied for reimbursing the travel expenses of persons under contract. The terms "contract" and/or "subcontract" have the same meaning as "grantee" and/or "subgrantee" where applicable.
 - a. Reimbursement for travel and/or per diem shall be at the rates established for nonrepresented/excluded state employees. Exceptions to California Department of Human Resources (CalHR) lodging rates may be approved by *the* Department of Health Care Services (DHCS) upon the receipt of a statement on/with an invoice indicating that State employee travel rates are not available.
 - b. Short Term Travel is defined as a 24-hour period, and less than 31 consecutive days, and is at least 50 miles from the main office, headquarters or primary residence. Starting time is whenever a contract or subcontract employee leaves his or her home or headquarters. "Headquarters" is defined as the place where the contracted personnel spends the largest portion of their working time and returns to upon the completion of assignments. Headquarters may be individually established for each traveler and approved verbally or in writing by the program funding the agreement. Verbal approval shall be followed up in writing or email.
 - c. Contractors on travel status for more than one 24-hour period and less than 31 consecutive days may claim a fractional part of a period of more than 24 hours. Consult the chart appearing on Page 2 of this document to determine the reimbursement allowance. All lodging reimbursement claims must be supported by a receipt*. If a contractor does not or cannot present receipts, lodging expenses will not be reimbursed.

(1) Lodging (with receipts*):

Travel Location / Area	Reimbursement Rate
Statewide (excluding the counties identified below)	\$ 90.00 plus tax
Counties of Napa, Riverside and Sacramento	\$ 95.00 plus tax
Counties of Los Angeles (excluding City of Santa Monica), Orange, Ventura and Edwards AFB	\$120.00 plus tax
Counties of Alameda, Monterey, San Diego, San Mateo and Santa Clara	\$125.00 plus tax
San Francisco County and the City of Santa Monica	\$150.00 plus tax

Reimbursement for actual lodging expenses that exceed the above amounts may be allowed with the advance approval of the Deputy Director of DHCS or his or her designee. Receipts are required.

*Receipts from Internet lodging reservation services such as Priceline.com which require prepayment for that service, ARE NOT ACCEPTABLE LODGING RECEIPTS and are not reimbursable without a valid lodging receipt from a lodging establishment.

(2) Meal/Supplemental Expenses: With substantiating receipts, a contractor may claim actual expenses incurred up to the following maximum reimbursement rates for each full 24-hour period of travel.

Meal / Expense	Reimbursement Rate
Breakfast	\$ 7.00
Lunch	\$ 11.00
Dinner	\$ 23.00
Incidental expenses	\$ 5.00

- d. Out-of-state travel may only be reimbursed if such travel is necessitated by the scope or statement of work and has been approved in advance by the program with which the contract is held. For out-of-state travel, contractors may be reimbursed actual lodging expenses, supported by a receipt, and may be reimbursed for meals and supplemental expenses for each 24-hour period computed at the rates listed in c. (2) above. For all out-of-state travel, contractors/subcontractors must have prior DHCS written or verbal approval. Verbal approval shall be confirmed in writing (email or memo).
- e. In computing allowances for continuous periods of travel of less than 24 hours, consult the chart appearing on Page 2 of this document.
- f. No meal or lodging expenses will be reimbursed for any period of travel that occurs within normal working hours, unless expenses are incurred at least 50 miles from headquarters.

2. If any of the reimbursement rates stated herein is changed by CalHR, no formal contract amendment will be required to incorporate the new rates. However, DHCS shall inform the contractor, in writing, of the revised travel reimbursement rates and the applicable effective date of any rate change.

At DHCS' discretion, changes or revisions made by DHCS to this exhibit, excluding travel reimbursement policies established by CalHR may be applied retroactively to any agreement to which a Travel Reimbursement Information exhibit is attached, incorporated by reference, or applied by DHCS program policy. Changes to the travel reimbursement rates stated herein may not be applied earlier than the date a rate change is approved by CalHR.

3. For transportation expenses, the contractor must retain receipts for parking; taxi, airline, bus, or rail tickets; car rental; or any other travel receipts pertaining to each trip for attachment to an invoice as substantiation for reimbursement. Reimbursement may be requested for commercial carrier fares; private car mileage; parking fees; bridge tolls; taxi, bus, or streetcar fares; and auto rental fees when substantiated by a receipt.
4. **Auto mileage reimbursement:** If a contractor uses his/her or a company car for transportation, the rate of reimbursement will be **57.5 cents** maximum per mile. If a contractor uses his/her or a company car "in lieu of" airfare, the air coach fare will be the maximum paid by the State. The contractor must provide a cost comparison upon request by the State. Gasoline and routine automobile repair expenses are not reimbursable.
5. The contractor is required to furnish details surrounding each period of travel. Travel expense reimbursement detail may include, but not be limited to: purpose of travel, departure and return times, destination points, miles driven, mode of transportation, etc. Reimbursement for travel expenses may be withheld pending receipt of adequate travel documentation.
6. Contractors are to consult with the program funding the contract to obtain specific invoicing procedures.

Per Diem Reimbursement Guide

Length of travel period	And this condition exists...	Meal allowed with receipt
Less than 24 hours	<ul style="list-style-type: none"> ▶ Trip begins at or before 6:00 a.m. and ends at or after 9:00 a.m..... ▶ Trip ends at least one hour after the regularly scheduled workday ends or begins at or before 4:00 p.m. and ends after 7:00 p.m. <p><i>Lunch or incidentals cannot be claimed on one-day trips.</i></p>	<p>Breakfast</p> <p>Dinner</p>
24 hours or more	<ul style="list-style-type: none"> ▶ Trip begins at or before 6:00 a.m..... ▶ Trip begins at or before 11:00 a.m..... ▶ Trip begins at or before 5:00 p.m..... 	<p>Breakfast</p> <p>Lunch</p> <p>dinner</p>
More than 24 hours	<ul style="list-style-type: none"> ▶ Trip ends at or after 8:00 a.m..... ▶ Trip ends at or after 2:00 p.m..... ▶ Trip ends at or after 7:00 p.m..... 	<p>Breakfast</p> <p>Lunch</p> <p>Dinner</p>
<p>The following meals may not be claimed for reimbursement: meals provided by the State, meals included in hotel expenses or conference fees, meals included in transportation costs such as airline tickets, or meals that are otherwise provided. Snacks and/or continental breakfasts such as rolls, juice, and coffee are not considered to be a meal.</p> <p>No meal expense may be claimed for reimbursement more than once in any given 24-hour period.</p>		

Exhibit H

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.

Exhibit H

HIPAA Business Associate Addendum

- 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

Exhibit H

HIPAA Business Associate Addendum

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.

Exhibit H

HIPAA Business Associate Addendum

3. **Security.** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
 - a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;
 - b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of 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:

Exhibit H

HIPAA Business Associate Addendum

- 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.

Exhibit H

HIPAA Business Associate Addendum

- 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.

Exhibit H

HIPAA Business Associate Addendum

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

Exhibit H

HIPAA Business Associate Addendum

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.

Exhibit H

HIPAA Business Associate Addendum

- 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 constitute 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.

Exhibit H

HIPAA Business Associate Addendum

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

Exhibit H

HIPAA Business Associate Addendum

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.

Exhibit H

HIPAA Business Associate Addendum

Attachment A

Business Associate Data Security Requirements

I. Personnel Controls

- A. *Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of 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.

Exhibit H

HIPAA Business Associate Addendum

- 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.

Exhibit H

HIPAA Business Associate Addendum

- 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.

Exhibit H

HIPAA Business Associate Addendum

- 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.

Exhibit I
Staffing Qualifications

Table of Contents

A. Senior/Executive Manager (Senior Management Staff) Qualifications and Responsibilities2

- 1. Enterprise Project Management Office (EPMO) Director2
- 2. Executive Director/Program Director (Contractor Representative).....3
- 3. Information Security Officer4
- 4. Privacy Officer (PO).....5
- 5. Operations Director6
- 6. Quality Management Director (QMD).....7
- 7. Systems Director7
- 8. Takeover Director (TOD)7

B. Representative Resume Staff Qualifications and Responsibilities8

- 1. Database Administrator8
- 2. Security Risk Assessor9
- 3. Manager.....10
- 4. Supervisor.....10

C. Technical Representative Resume Staff Qualifications and Responsibilities.....11

- 1. Systems Analyst.....11
- 2. Programmer11
- 3. Liaison.....13

D. Qualification Requirements14

Exhibit I
Staffing Qualifications

The Contractor shall be responsible for meeting and maintaining the personnel staffing resources that meet the minimum qualifications and job duties as described in this exhibit. The Department of Health Care Services (DHCS) reserves the right to renegotiate the following staffing positions after the Contract is executed. If the same Contractor is awarded the Administrative Services Organization (ASO) Contract and the Fiscal Intermediary (FI) Contract, then it shall only staff one of any named senior management staff positions that are identified in both Contracts. These staffing positions include varying levels, Contractor staff positions listed by functional title and/or position name, minimum qualifications required by the State, and job duties and/or responsibilities.

Exhibit E, Additional Provisions Contractor Resource Levels, defines additional requirements for the Contractor staff positions included in this exhibit.

Functional Position Title	Category
Senior Management Team	
Enterprise Project Management Office (EPMO) Director	Sr/Exec
Executive Director/Program Director (Contractor Representative)	Sr/Exec
Information Security Officer	Sr/Exec
Privacy Officer (PO)	Sr/Exec
Operations Director	Sr/Exec
Quality Management Director (QMD)	Sr/Exec
Systems Director	Sr/Exec
Takeover Director (TOD)	Sr/Exec
Representative Resume Staff Positions	
Database Administrator	Representative Resume
Security Architect	Representative Resume
Security Risk Assessor	Representative Resume
Managers	Representative Resume
Supervisor	Representative Resume
Technical Representative Staff Positions	
Systems Analyst	Technical Representative Resume
Senior Programmer	Technical Representative Resume
Advanced Programmer	Technical Representative Resume
Associate Programmer	Technical Representative Resume
Apprentice Programmer	Technical Representative Resume
Entry Programmer	Technical Representative Resume
Liaison	Technical Representative Resume

Exhibit I
Staffing Qualifications

A. Senior/Executive Manager (Senior Management Staff) Qualifications and Responsibilities

Senior/Executive Management staff, referenced throughout the Contract as Senior Management Staff, shall be those individuals assigned to the positions listed in the table above, and shall have the following minimum qualifications, education and responsibilities. At the discretion of the Contracting Officer, relative work experience may be substituted for the required college education on a two for one basis.

1. Enterprise Project Management Office (EPMO) Director

- a. **Qualifications:** Shall have at least ten (10) years' relevant experience and five years of experience in an administrative or consultative capacity in a business service program, at least two years of which shall have included responsibility for Service-Oriented Architecture (SOA) principles and practices. Previous experience with a government or private sector healthcare payer program in management methodology, processes and tools, system architecture and design, and strategic planning and execution. A minimum of five years' experience in data processing, hardware platforms, enterprise software applications and outsourced systems including a good understanding of computer systems characteristics, features and integration capabilities; focus on program management and/or project management; successful experience in managing complex projects and/or programs to completion; demonstrated knowledge in business process modeling, systems design, development, documentation, testing, implementation and/or maintenance, (i.e.; System Development Life Cycle (SDLC) ranging from business requirements through implementation).
- b. **Education:** A Bachelor's degree in Computer Science, Computer Information Systems, Management Information Systems, Engineering or a related field is required. Two years' additional management experience in a government or private sector healthcare payer claims payment processing, or in a Medicaid Management Information Systems (MMIS) environment may substitute for the degree on a two for one basis.

One or more of the following certifications:

- 1) Project Management Professional (PMP)
 - 2) Certified Business Analysis Professional (CBAP)
 - 3) Certified Information Systems Auditor (CISA)
 - 4) Certified Information Systems Security Professional (CISSP)
- c. **Additional Experience:**
- 1) Three or more years' experience in all of the following knowledge areas of the Project Management Institute's (PMI's) Project Management Body of Knowledge (PMBOK):

Exhibit I
Staffing Qualifications

- a) Integration Management
 - b) Scope Management
 - c) Cost Management
 - d) Time Management
 - e) Quality Management
 - f) Communications Management
 - g) Human Resources Management
 - h) Risk Management
 - i) Stakeholder Management
 - j) Procurement Management
- 2) Applied knowledge of business theory, business processes, management, budgeting and business office operations
 - 3) Proven technical and functional problem solving, tracking and resolution skills
 - 4) Ability to manage complex projects
 - 5) Excellent verbal, written and presentation communication skills
 - 6) Experience in program management or project management in both government and healthcare environments
 - 7) Ability to work effectively with technical and non-technical managerial and professional staff demonstrated through experience
 - 8) Medicaid Information Technology Architecture (MITA) experience
- d. **Responsibilities:** The primary point of contact with the State's Contracting Officer for all activities related to Contract administration including, but not limited to, compliance with all Contract terms and conditions. Principal officer responsible for the operation of the EPMO.

2. Executive Director/Program Director (Contractor Representative)

- a. **Qualifications:** Extensive managerial and program administrative experience to include responsibility for a combination of management functions such as program planning, policy formulation, organization coordination and control, and fiscal management. Requires effective communication, organization, and prioritization skills and proven ability to direct and motivate the workforce. A minimum of five years of experience managing a large scale health contract with

Exhibit I
Staffing Qualifications

a government or private sector healthcare payer. Knowledge of Medicaid and Medicare regulations and standards as well as cost reporting, profit and loss, and budget compliance is required.

- b. **Education:** Shall have at least a Bachelor's degree in Healthcare Administration, Business Administration/Management, Finance or related field, a clinical specialty or equivalent. Master's degree in one of these fields preferred.
- c. **Responsibilities:** The primary point of contact with the State's Contracting Officer for all activities related to Contract administration including, but not limited to, compliance with all Contract terms and conditions. Shall ensure the maintenance of adequate staffing levels to meet all State requirements and deliverables. Shall oversee all project management, scheduling, correspondence between the State and Contractor, dispute resolution, personnel issues with Contractor staff and status reporting to the State. Oversee the implementation of all quality assurance criteria and reviews to ensure Contract compliance and fulfillment of performance objectives. Also leads and coordinates the Contractor's implementation activities, including implementation evaluation, training, coaching, mentoring, reporting, and recommendation activities.

3. Information Security Officer

- a. **Qualifications:** Shall have a minimum of five years' experience in computing or related area, with a focus on information security, technology, management and policy; experience in the development and implementation of planning security policy, procedure, and/or safeguards; extensive knowledge of security administration and computer security tools; successful experience in retrieving, analyzing, reporting, addressing and /or tracking security intrusions and vulnerabilities; demonstrated knowledge in systems design, development, documentation, testing, implementation and/or maintenance; demonstrated ability to work effectively with technical and non-technical managerial and professional staff. Two years' additional management experience in a government or private sector healthcare payer claims payment processing, or in a Medicaid Management Information System (MMIS) environment may substitute for the degree on a two for one basis.
- b. **Education:** A Bachelor's degree in Computer Science, Computer Information Systems, Management Information Systems, Business Administration, Public Policy, Law or a related field is required. CISSP Certification required.

Additional Storage Area Network (SAN) certification desired:

- 1) Security + Cisco Certified Internetwork Expert (CCIE), Certified Wireless Security Professional(CWSP)
- 2) CISA
- 3) Global Information Assurance Certificate (GIAC)

Exhibit I
Staffing Qualifications

- 4) Systems Security Certified Practitioner (SSCP)
- 5) Certified Ethical Hacker.

c. **Additional Experience:**

- 1) Three or more years' experience in at least three of the following domains in the CISSP certificate:
 - a) Access control systems and methodology
 - b) Application and systems development security
 - c) Business continuity planning and disaster recovery planning
 - d) Cryptography of law, investigation and ethics
 - e) Operations security
 - f) Security architecture and models
 - g) Security management practices
 - h) Telecommunications and networking
- 2) Proven technical and functional problem solving, tracking and resolution skills
- 3) Ability to manage complex projects
- 4) Excellent verbal, written and presentation communication skills
- 5) Experience in technology management or information security in both government and healthcare environments

- d. **Responsibilities:** Principal Officer with responsibility for ensuring the Contractor's adherence to the FI Contract's Information Security Office provisions including compliance with all applicable legal, statutory and regulatory requirements. The Contractor shall supply all necessary staff to perform the duties of the Information Security Office.

4. Privacy Officer (PO)

- a. **Qualifications:** Shall have a minimum of five years' experience in privacy activities that included overseeing the establishment, implementation and adherence to policies on patient privacy, confidentiality and release of patient information; experience developing, conducting and reporting privacy risk assessments and internal privacy audits; experience overseeing the development and delivery of privacy training and awareness in a government and/or healthcare setting. Additional relevant management experience may substitute for the degree on a two for one basis.

Exhibit I
Staffing Qualifications

- b. **Education:** Formal education equivalent to a Bachelor's degree in Public Administration, Business Administration, or a related field is required.

One or more of the following certifications:

- 1) PMP
- 2) GIAC
- 3) SSCP
- 4) CISA
- 5) CISSP

- c. **Additional Experience:**

- 1) Four years' experience in program organization and administration
- 2) Excellent verbal, written and presentation communication skills
- 3) Experience managing patient privacy disputes and requests for changes to their health record
- 4) Application of knowledge and understanding of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy Rule
- 5) Application of knowledge of standard audit procedures

- d. **Responsibilities:** Principal Officer with responsibility for ensuring the Contractor's adherence to the FI Contract's Privacy Office provisions.

5. Operations Director

- a. **Qualifications:** Shall have a minimum of four years' experience managing fiscal intermediary or healthcare claims processing operations and personnel with a government or private sector healthcare payer, including a minimum of two years' MMIS experience. Supervisory/administrative experience in the execution and/or evaluation of program policies. Excellent verbal, written and presentation communications skills. Additional relevant management experience may substitute for the degree on a two for one basis.
- b. **Education:** A Bachelor's degree in related field.
- c. **Responsibilities:** Principal Officer over the Contractor's claim processing operations.

Exhibit I
Staffing Qualifications**6. Quality Management Director (QMD)**

- a. **Qualifications:** Shall have a minimum of five years' quality management experience for a government or healthcare payer, including experience during implementation and testing of a new claims payment system. Extensive program administrative experience; strong exposure to Quality Management and Quality Assurance processes and ability to apply these processes to ensure including the accuracy and timeliness of a Contractor's performance in each area of responsibility. Excellent verbal, written and presentation communication skills. Additional relevant management experience may substitute for the degree on a two for one basis.
- b. **Education:** A Bachelor's degree in Computer Science or a related field is required.
- c. **Responsibilities:** Principal Officer with responsibility for ensuring the Contractor adheres to the FI Contract's Quality Management provisions. Communication and dissemination of quality assurance and improvement information throughout all levels of Contractor Operations and concurrently to the Contracting Officer.

7. Systems Director

- a. **Qualifications:** Shall have a minimum of four years of experience for a Medicaid or other private sector or government healthcare payer in: management methodology, processes and tools; systems architecture and design; strategic planning and execution. Substantial exposure to data processing, hardware platforms, enterprise software applications and outsourced systems including: good understanding of computer systems characteristics, features and integration capabilities; SOA principles and practices and experience with SDLC from business requirements through implementation. Proven experience in program and project management, planning, organization, budgeting, risk mitigation, development and implementation in a state of similar scope and size as California. Excellent verbal, written and presentation communications skills. Additional qualifying management experience may substitute for the required education on a two for one basis.
- b. **Education:** A Bachelor's degree in Computer Science or a related field is required. PMP certification from the PMI and/or Master's degree in one of these fields preferred.
- c. **Responsibilities:** Principal Officer overseeing the Contractor's Systems Group.

8. Takeover Director (TOD)

- a. **Qualifications:** Shall have lead management experience in the transfer of responsibility for an MMIS or other large government or private sector healthcare payer existing system from a predecessor contractor to a successor contractor. Shall be knowledgeable of and adhere to project management methods and standards which are based upon the PMI PMBOK, Institute of Electrical and Electronics Engineers (IEEE) and industry best practices. Must have a general

Exhibit I Staffing Qualifications

knowledge of data processing concepts, practices, methods and principles, including SDLC. Shall have excellent verbal, written and presentation communications skills.

- b. **Education:** A Bachelor's degree in Business Administration, Computer Science or a related field is required.
- c. **Responsibilities:** As principal management lead, shall be responsible for Takeover of the current California Dental Medicaid Management Information System (CD-MMIS). Shall ensure close alignment between all stakeholders from initiation through close-out of all Takeover activities detailed in the Contract, Exhibit A, Attachment I. Shall adhere to project management guidelines as contained within the Statewide Information Management Manual (SIMM) and ensure Information Technology (IT) project alignment and compliance with State direction, rules and regulations to deliver all Takeover requirements within approved baselines for scope, schedule and budget. Responsible for successful completion of all Takeover requirements as defined in the Contract Scope of Work (SOW).

B. Representative Resume Staff Qualifications and Responsibilities

Representative Resume staff shall be those individuals assigned to the positions listed in the table above and shall have the following minimum qualifications and responsibilities. Work experience may be substituted for the required college education as indicated in the qualification requirements listed below for each position on a two for one basis.

1. Database Administrator

- a. **Qualifications:** Minimum of two years of progressively responsible, full-time work experience above the trainee level in database management system administration. Experience in the utilities and operations of a database management system. Experience in development and enforcement of policies, procedures and standards to promote consistency of systems development in the data repository. Requires excellent oral and written communication skills and ability to work cooperatively with others.
- b. **Education:** Shall have a four year college degree or equivalent work experience.
- c. **Responsibilities:** Shall be responsible for all aspects of a data base management system environment including all new development. Develop data models for applications using deliverables from the SDLCs Definition phase that accurately support the customer's business requirements. Applied knowledge of data base access methods (e.g., virtual storage access method) to select appropriate configuration parameters for efficient storage and retrieval of the data. Recommends use of new functionality from data base management releases to take advantage of new features. May develop and analyze data distribution design alternatives consistent with the enterprise business and technical direction. Shall maintain and manage the data dictionary and data model within the database. Analyzes space requirements to project the amount

Exhibit I
Staffing Qualifications

of storage resources required. Documents the data base design to ensure that data base specifications are understood and used properly by the application. Shall maintain currency with continuously evolving healthcare practices, equipment and technology.

- d. **Additional Qualifications:** Ability to apply knowledge of logical data models to implement a customer's business rules into the physical design of the database. Applies knowledge of data base design to identify impact on the performance and maintainability of the application system.

2. Security Risk Assessor

- a. **Qualifications:** Shall have a minimum of eight years of experience in the field of Information Security, Information Security Risk Assessment or IT audit. Broad range of technology experience to include: Z/OS, UNIX, Windows Server 2003/2008/2012, Intrusion detection systems, TCP/IP, Secure Application Programming. At least five years of experience implementing security controls. Experience in a variety of complex architecture projects, able to lead and direct other architects in all phases of enterprise-wide architecture development projects and/or initiatives. Experience with new architectural approaches such as SOA. Substantial exposure to data processing, hardware platforms, enterprise software applications and outsourced systems including a good understanding of computer systems characteristics, features and integration capabilities and experience with SDLC from business requirements through implementation. Proven experience in program and project management, planning, organization, risk mitigation, development and implementation. Knowledge and experience with network and host-based security strategies and methodologies; risk assessments and analysis; incident response; information security awareness and education; and a strong technical background with experience and knowledge of allocation layer security, knowledge of operating systems, networking protocols, intrusion detection/protection, active content, malware, defense in depth. Must have excellent communication skills, verbal and written, including the ability to create, plan and organize effective presentations. Good interpersonal skills as demonstrated by working in a collaborative environment. Additional relevant management experience may substitute for the degree on a two for one basis.
- b. **Education:** Bachelor's Degree in Computer Science, Business Administration/Management or related field. Master's degree in one of these fields preferred.
- c. **Responsibilities:** Shall ensure all IT decisions are made with consideration of security and risk impact on the entire CD-MMIS system. Provide innovative strategic technology direction for CD-MMIS and oversight of technology projects. Define approaches for technology including SOA design and development, web services, commercial, off-the-shelf (COTS) products, middleware tools, productivity tools and Web technologies. Develop plans and strategies to reduce/mitigate risks to CD-MMIS.

Exhibit I
Staffing Qualifications

- d. **Additional Qualifications:** Knowledge of and experience in HIPAA, CISA, CISSP or SANS certification. Knowledge of and experience in National Institute of Standards and Technology (NIST) and Centers for Medicare and Medicaid Services (CMS) security standards.

3. Manager

- a. **Qualifications:** Shall possess a minimum of five years' increasingly responsible experience leading, developing, coaching and managing a staff for a government or private sector healthcare payer, including a minimum of two years MMIS experience in a state of an equivalent scope to California. Demonstrated record of: delivering high levels of client service; establishing objectives and plans for the organization's operation; controlling activities through subordinate managers or by direct supervision; developing, administering and controlling the budget for the organization; evaluating the performance of subordinates; administering compensation; and maintaining appropriate staffing levels. Shall have effective communication, organization and prioritization skills and proven ability to direct and motivate the workforce. Shall possess detailed working knowledge of Medicare and/or Medicaid regulations and standards. Shall have detailed working knowledge of industry standards, area of study fundamentals and best practices relative to the role assignment area.
- b. **Education:** Completed four years of college. Shall have attained higher education degree(s) and shall possess current professional certification(s) and/or license(s). Shall have completed or be in the process of completing course work focusing on: leadership decision making; personnel management, including staff performance planning, coaching and corrective actions; salary and expense tracking as part of the budget forecasting process; and written and verbal communications skills. Increased relative work experience, completed managerial course training and demonstrated accomplishments may be substituted for a degree.
- c. **Certifications/Licenses:** Shall have obtained professional certification(s) and/or license(s) relative to the position. Increased relative work experience and demonstrated accomplishments may be substituted for professional certification(s) and/or license(s) unless the duties performed require specific certification or licensure pursuant to State laws.

4. Supervisor

- a. **Qualifications:** Shall have a minimum of two years' relative work experience in their assigned field, at least one year of which must have been in a supervisory capacity. Shall possess detailed working knowledge of Medicare and/or Medicaid regulations and standards, including detailed working knowledge of industry standards, area of study fundamentals and best practices relative to the role assignment area.
- b. **Education:** Shall have completed or be in the process of completing course work focusing on personnel management, including staff performance planning, coaching and corrective actions, and written and verbal communication skills

Exhibit I
Staffing Qualifications

- c. **Certifications/Licenses:** Shall have obtained professional certification(s) and/or license(s) relative to the position. Increased relative work experience and demonstrated accomplishments may be substituted for education.

C. Technical Representative Resume Staff Qualifications and Responsibilities

Proposed organizations shall have a blend of resources sufficient to support DHCS business needs, including business analysts, technical writers, project managers, system designers, testers, programmers, database administrators, and an appropriate level of managerial, supervisory and administrative / clerical support staff. Technical Representative Resume staff shall be those individuals assigned to the positions listed in the table above and shall have the following minimum qualifications and responsibilities.

1. Systems Analyst

Shall have four years of progressively responsible, full-time work experience above the trainee level in the electronic data processing systems study, design or programming (at least one of the four years' experience must have been spent working in a COBOL or Client Server Application development environment), project responsibility for analyzing operational methods and designing computer systems to meet desired results. Good interpersonal skills as demonstrated by working in a collaborative environment.

2. Programmer

Shall have four years of progressively responsible, full-time work experience above the trainee level in the electronic data processing systems study, design or programming (at least one of the four years' experience must have been spent programming in a COBOL or Client Server Application development environment), project responsibility for analyzing operational methods and developing computer programs to meet desired results. Good interpersonal skills as demonstrated by working in a collaborative environment.

a. Senior

- 1) **Qualifications:** Shall, in addition to the minimum qualifications for Associate and Advanced levels (when applicable), possess superior education, professional certification(s) and/or license(s), have relative work experience in their assigned field for a minimum of five years for a government or private sector healthcare payer. Work experience shall include functions such as team lead, internal and external communications, organization and prioritization skills and proven ability to deliver quality products and services while meeting deliverables objectives. Shall possess detailed working knowledge of Medicare and/or Medicaid regulations and standards. Shall have detailed working knowledge of industry standards, area of study fundamentals and best practices relative to the role assignment area.
- 2) **Education:** Shall have a Bachelor level degree from an accredited four-year university, college or technical institute. Other completed relative courses of study and/or increased relative work experience and demonstrated

Exhibit I
Staffing Qualifications

accomplishments may be substituted for a degree on a two for one basis, with Contracting Officer's prior written approval.

- 3) **Certifications/Licenses:** Shall have obtained professional certification(s) and/or license(s) relative to the position. Increased relative work experience and demonstrated accomplishments may be substituted for professional certification(s) and/or license(s).

b. Advanced

- 1) **Qualifications:** Demonstrated competency in an Associate role for at least one year, and completed specialized training and demonstrated competency for at least one year in using systems tools relative to the position that enable the staff member to perform enhanced functions relative to the area assigned. This includes, but is not limited to, reporting tools, data mining tools, database management tools, statistical measuring tools, process design tools and others.

c. Associate

- 1) **Qualifications:** Possess required education level and required professional certification(s) and/or license(s). Have required breadth of knowledge and relative work experience in their assigned field for a minimum of two years. Shall possess working knowledge of Medicare and/or Medicaid regulations and standards. Shall have working knowledge of industry standards, area of study fundamentals and best practices relative to the role assignment area.
- 2) **Education:** For non-technical positions the staff member shall have completed all baseline training courses for the relative area of work. For technical positions the staff member shall be currently enrolled in and have completed at least seventy-five percent (75%) of studies leading to a Bachelor level degree from an accredited four-year university, college or similar technical institute, in a field of study relative to the work area the individual will Apprentice. Other completed relative courses of study may be substituted for a degree, with Contracting Officer's prior written approval.
- 3) **Certifications/Licenses:** Shall be pursuing and have completed at least fifty percent (50%) of course segments leading to professional certification(s) and/or license(s) relative to the position. Increased relative work experience and demonstrated accomplishments may be substituted for these professional certification(s) and/or license(s) requirements.

d. Apprentice

- 1) **Qualifications:** Shall possess a minimum of one year of experience in a work area relative to the area, have a working knowledge for the position, possess working awareness of Medicare and/or Medicaid regulation and standards, and have a working awareness of industry standards, area of study fundamentals and best practices relative to the role assignment area.

Exhibit I
Staffing Qualifications

- 2) **Education:** Shall have completed or nearly completed education requirements. For non-technical positions the staff member shall have completed or be currently enrolled in training courses for the relative area of work. For technical positions the staff member shall be currently enrolled in and have completed at least fifty percent (50%) of studies leading to a Bachelor-level degree from an accredited four-year university, college or similar technical institute, in a field of study relative to the work area the individual will Apprentice. Other completed relative courses of study may be substituted.
- 3) **Certifications/Licenses:** Shall be pursuing and have completed at least twenty-five percent (25%) of course segments leading to professional certification(s) and/or license(s) relative to the position. Increased relative work experience and demonstrated accomplishments may be substituted for these professional certification(s) and/or license(s) requirements.

e. Entry

- 1) **Qualifications:** Satisfactorily meet attitude and aptitude testing requirements during the interview selection process for the position. Entry level may not be used as a job classification designation for hourly reimbursed positions.
- 2) **Education:** Shall have completed high school or obtained a General Education Degree (GED) certificate. Increased relative work experience and demonstrated accomplishments may be substituted for a high school diploma or GED certificate, with Contracting Officer's prior written approval.
- 3) **Certifications/Licenses:** Shall have obtained professional certification(s) and/or license(s) relative to the position (e.g., Typing Certificate). Increased relative work experience and demonstrated accomplishments may be substituted for professional certification(s) and/or license(s).

3. Liaison

- a. **Qualifications:** Two years of experience in dental billing and claims processing environment. Such staff shall be knowledgeable of Treatment Authorization Request (TAR) processing, dental claims processing, quality management, research and audit activities, and fully trained in every aspect of the operations prior to performing the task. Shall possess working knowledge of Medicare and/or Medicaid regulations and standards. Shall have working knowledge of industry standards, area of study fundamentals and best practices relative to the role assignment area.
- b. **Education:** Two years of dental office experience or graduation from an accredited dental assistant school.

Exhibit I
Staffing Qualifications

D. Qualification Requirements

Individuals filling Contractor staff positions required in the Contract shall have acquired some portion of the experience required in the qualifications defined above and elsewhere in the Contract within the past five years from the first day of Takeover or from the date the position is filled during the term of the Contract, whichever date is most recent.

Included with the staff position resumes submitted to the State, the Contractor shall provide supporting information that substantiates each individual's experience and knowledge is commensurate with or scalable to that individual satisfactorily performing in an MMIS of California's size and complexity.

Professional certifications and/or licenses required in the Contract shall be current, from the State of California or other approved government jurisdiction, not under suspension from CMS or from practice in California, and not previously sanctioned for fraud or abuse.

The Contractor shall assure that all staff assigned to the Contract meets the minimum qualification requirements defined in the Contract for all Contractor positions. These minimum qualification requirements apply to Contractor staff specifically identified in the requirements of the Contract to additional staff the Contractor identifies in its Narrative Proposal response, and/or subsequently determines to be necessary to its satisfactorily meeting the requirements of the Contract.

Except where specifically defined differently elsewhere in the Contract, the Contractor shall assure that all Contractor positions are defined to include one or an equivalent of the required job classification designations and shall meet the minimum qualifications associated with each. In all deliverables the Contractor submits to the State that includes Contractor staffing, the Contractor shall include these job classification designations. Exceptions to these requirements require prior written approval by the Contracting Officer.