35256

MEDI-CAL TARGETED CASE MANAGEMENT PROVIDER PARTICIPATION AGREEMENT

Name of Provider: The City of Long Beach PPA # 61-19EVRGRN

ARTICLE I – STATEMENT OF INTENT

This Provider Participation Agreement (PPA) constitutes the entire agreement between the Provider and the California Department of Health Care Services (DHCS) regarding Targeted Case Management (TCM) services and is subordinate to the Medi-Cal Provider Agreement (DHCS Form 6208) entered into by the Provider in conjunction with the Provider's enrollment in the Medi-Cal Program. To the extent a prior agreement exists, this PPA replaces all prior PPAs.

ARTICLE II- AUTHORITY

This PPA establishes the responsibilities of a California qualified Local Governmental Agency (LGA or Provider) and DHCS, for the provision of TCM services to eligible Medi-Cal beneficiaries, pursuant to Welfare and Institutions Code section 14132.44. Provider shall be an entity located and operating in the State of California.

ARTICLE III – TERM AND TERMINATION OF THE AGREEMENT

This PPA is effective **July 1, 2019**, and shall continue in full force and effect until terminated by either party.

Termination without Cause: Either party may terminate this PPA by providing the other party with 30 days advance written notice of intent to terminate. Termination under this paragraph shall result in Provider's immediate disenrollment from the TCM Program on the termination date and exclusion without formal hearing under the California Administrative Procedure Act (APA) from further participation in the TCM Program unless and until Provider is re-enrolled by DHCS in the TCM Program.

Termination for Cause: This PPA shall be automatically terminated if the Provider's DHCS Form 6208 and Medi-Cal Disclosure Statement form 6207 are terminated or Provider is suspended from Medi-Cal under the terms of the DHCS Form 6208, respectively. This PPA's automatic termination or suspension shall be effective the same date as the Provider's DHCS Form 6208 and Medi-Cal Disclosure Statement form 6207 termination from Medi-Cal. Termination under this paragraph will result in Provider's immediate disenrollment and exclusion without formal hearing under the APA from further providing services under the TCM Program. Additionally, DHCS shall have the authority to automatically terminate this PPA if a conflict of interest is determined to exist by DHCS and cannot be adequately resolved to the satisfaction of DHCS pursuant to Article X of this PPA.

ARTICLE IV – PROJECT REPRESENTATIVES

A. The contact persons during the term of this PPA are:

Department of Health Care Services	**Provider**
Shelly Taunk, Chief County-Based Claiming and Inmate Services Section Telephone: (916) 345-7934 Fax: (916) 324-0738 Email: Shelly.Taunk@dhcs.ca.gov	Name: Nancy Riano, Nursing Services Officer Telephone: (562) 570-4254 Fax: (562) 570-4099 Email: Nancy.Riano@longbeach.gov

B. Direct all inquiries to:

Department of Health Care Services	**Provider**
County-Based Claiming and Inmate Services Section Targeted Case Management Unit Attention: Sara Schmid, Chief Suite 71.3024, MS 4603 P.O. Box 997436 Sacramento, CA, 95899-7436 Telephone: (916) 345-7691 Fax: (916) 324-0738 Email: DHCS-TCM@dhcs.ca.gov	Name: Denise Tong City of Long Beach Depaertment of Health and Human Services 2525 Grand Avenue, Long Beach, CA 90815 Telephone: (562) 570-4278 Fax: (562) 570- 4099 Email: Denise.Tong@longbeach.gov

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

ARTICLE V – PROVIDER RESPONSIBILITIES

By entering into this PPA, the Provider agrees:

A. To comply with all provisions of the Medi-Cal Provider Manual, the CMAA/TCM Time Survey Methodology, DHCS Policy and Procedure Letters (PPLs), DHCS issued policy directives, TCM Cost Report Instructions Manual, the California Medicaid State Plan as it pertains to TCM services, all as periodically amended.

B. To ensure all applicable state and federal requirements are met with regard to expense allowability and fiscal documentation:

1. Any TCM Summary Invoices received from a Provider, and accepted or submitted for payment by DHCS, shall not be deemed evidence of allowable agreement costs.

2. Supporting documentation of all expenses incurred and amounts invoiced shall be maintained for review and audit, and supplied to DHCS upon request, pursuant to this PPA to permit a determination of expense allowability.

    a. If the allowability or appropriateness of an expense cannot be determined by DHCS because the invoice detail, fiscal records, or backup documentation is nonexistent or inadequate, according to generally accepted accounting principles or practices, all questioned costs may be disallowed and payment may be withheld or recouped by DHCS. Upon receipt of adequate documentation supporting a disallowed or questioned expense, reimbursement may resume for the amount substantiated and deemed allowable.

C. That the TCM providers and their subcontractors are considered contractors solely for the purposes of U.S. Office of Management and Budget (OMB) Uniform Guidance. (2 Code of Federal Regulations (C.F.R.) § 200, and specifically, 2 C.F.R. § 200.330) Consequently, as a contractor, as distinguished from sub-recipient, a Dun and Bradstreet Universal Numbering System (DUNS) number is not required.

D. That the Provider's LGA Coordinator is responsible for working directly with DHCS in requesting MEDSLITE access for the Provider's (county or city) TCM staff. The Provider can have no more than three users with access to MEDSLITE. The LGA Coordinator is responsible for maintaining an active list of users for MEDSLITE and collecting a signed Oath of Confidentiality from each user. The Provider's LGA Coordinator is responsible for ensuring users are informed they cannot share user accounts, that MEDSLITE is to be used for only authorized purposes, and that all activity is logged. DHCS will only accept account requests from an authorized Provider's LGA Coordinator. DHCS may deny access to MEDSLITE at its discretion.

    1. The Provider's LGA Coordinator will provide, assign, delete, and track user accounts to authorized TCM staff members upon request.

    2. The Provider's LGA Coordinator is responsible for ensuring processes are in place, which result in prompt MEDSLITE account deletion requests when users leave employment or no longer require access due to a change in job duties. The Provider's LGA Coordinator must perform a monthly reconciliation to identify account termination, process violations, and ensure corrective actions are implemented.

E. That by November 1 of each year the Provider shall:

    1. Submit via electronic mail (e-mail) an annual TCM Cost Report for the service period of the preceding July 1 through June 30 to dhsaitcm@dhcs.ca.gov.

        a. E-mail submissions of the TCM Cost Report shall include the following completed documents:

1. Completed Cost Report Template signed and scanned (PDF)

2. Completed Cost Report Template (Excel)

3. LGA certification page signed and scanned (PDF)

4. Non-LGA Local Public Entities (LPE) Certification and LGA Attestation Statements for the TCM Cost Report signed and scanned (PDF), if applicable.

b. Each e-mail submission shall follow the examples below when naming the electronic files for the e-mail submission of the TCM Cost Report:

Examples:

2013 Santa Cruz CR.xls (Fiscal Year [FY] 2013-14 Santa Cruz Cost Report, Excel version)

2013 Santa Cruz CR.PDF (FY 2013-14 Santa Cruz Cost Report, signed and scanned PDF version)

c. Each e-mail submission shall follow the example below when naming the e-mail for the submission of the TCM Cost Report:

Example:

Name of LGA, LGA Code, Fiscal Year End Date (FYE), Part xx
Santa Cruz County, 44, FYE 063014, Part 1 of 3

F. To accept payments as reimbursement in full as received for TCM services pursuant to this PPA. Payments are subject to review and audit by both DHCS and the Centers for Medicare and Medicaid Services.

G. To submit TCM Summary Invoices in accordance with 42 Code of Federal Regulations part 433.51, California Code of Regulations, title 22, sections 51185, 51271, 51272, 51351, 51351.1, 51365, 51535.7, and 51492, and ensure TCM Summary Invoices are post-marked within 12 months from the date of service.

H. To execute a Memorandum of Understanding (MOU) with Medi-Cal Managed Care Health Plan(s) (MCPs) serving beneficiaries in the same county as the Provider when the Provider is in a participating MCP in accordance with state issued policy directives, including PPLs and federal directives, all as periodically amended. The MOU will serve to define the respective responsibilities between Provider's TCM Program and MCPs and must include coordination protocols to ensure non-duplication of services provided to beneficiaries in common.

I. That in addition to the Annual Participation Prerequisite (APP) required documentation due annually, Provider will submit the additional documents listed below:

- A list of the Provider's TCM case managers' names and National Provider Identification (NPI) numbers.

- Proof displaying verification of case managers not on the Office of Inspector General List of Excluded Individuals Exclusion (OIG LEIE) list. The Provider can satisfy this requirement by submitting electronic screenshots.

ARTICLE VI – DHCS RESPONSIBILITIES

By entering into this PPA, DHCS agrees to:

A. Establish an all-inclusive interim rate for the Provider to claim for TCM services.

B. Provide the TCM Program with inquiry-only MEDSLITE accounts. Providers will use MEDSLITE accounts to perform aid code verification for the Affordable Care Act (ACA) encounters billed through TCM.

C. Perform settlement reconciliation to reflect the actual costs the Provider incurred in providing TCM services to Medi-Cal beneficiaries.

D. Review and process TCM Summary Invoices within 24 months from the date of service. Upon review, processing, and approval of valid TCM encounters, DHCS shall schedule TCM Summary Invoices for payment.

E. Provide training and technical assistance to enable the Provider to identify costs related to proper invoicing documentation and billing procedures. DHCS will provide oversight to ensure compliance with Welfare and Institutions Code section 14132.44 and all other governing federal and state laws and regulations.

F. Conduct the reviews listed below annually for both currently enrolled providers and all newly enrolled providers to prevent Payment Error Rate Measurement (PERM) findings:

1. DHCS will verify that the NPI numbers of TCM case managers working for a Provider are active on an annual basis. If a NPI number of a TCM case manager is no longer active, DHCS will contact the Provider and inform them that the ineligible TCM case manager cannot provide TCM services. Once the TCM case manager's NPI has returned to an active status, the Provider must contact DHCS. At that point, DHCS will re-determine the TCM case manager's eligibility to participate in TCM.

2. DHCS will review and verify the State Administrative Manual (SAM) for existing entity registration records or exclusion records of TCM providers.

ARTICLE VII – FISCAL PROVISIONS

Reimbursement to Provider shall be made pursuant to this PPA in the following manner:

A. Upon the Provider's compliance with all provisions pursuant to Welfare and Institutions Code section 14132.44, California Code of Regulations, title 22, division 3 (commencing with section 50000), and this PPA, and upon the submission of a TCM Summary Invoice, based on valid and substantiated information, DHCS agrees to process the TCM Summary Invoice for reimbursement.

B. Transfer of funds to Providers for reimbursement is contingent upon the availability of Federal Financial Participation (FFP).

C. The Provider shall verify the Certified Public Expenditures (CPE) from the Provider's General Fund, or from any other funds allowed under federal law and regulation, for Title XIX funds claimed for TCM services performed pursuant to Welfare and Institutions Code section 14132.44. DHCS shall deny payment of any TCM Summary Invoice submitted under this PPA, if DHCS determines that the certification is not adequately supported for the purposes of claiming FFP. Expenditures certified for TCM costs shall not duplicate, in whole or in part, claims made for the costs of direct patient services or services paid by other Medi-Cal eligible programs.

D. Failure to timely submit cost reports, or other documents used to verify CPE, by the Provider within the statutory, regulatory, or contractual deadline shall entitle DHCS to declare any funds paid to the Provider for the cost report period as an overpayment and allow DHCS to recoup the funds.

ARTICLE VIII – BUDGET CONTINGENCY CLAUSE

A. It is mutually agreed that if the Budget Act for the current State Fiscal Year (SFY) or any subsequent SFYs covered under this PPA does not appropriate sufficient funds for the TCM Program, this PPA shall be of no further force and effect. In this event, DHCS shall have no liability to pay any funds whatsoever to the Provider or to furnish any other considerations under this PPA and the Provider shall not be obligated to further provide services under the TCM Program.

B. If funding for any SFY is reduced or deleted by the Budget Act for purposes of the TCM Program, DHCS shall have the option to either cancel this PPA, with no liability occurring to DHCS, or offer an agreement amendment to the Provider to reflect the reduced amount.

ARTICLE IX – LIMITATION OF STATE LIABILITY

A. Notwithstanding any other provision of this PPA, DHCS shall be held harmless from any federal audit disallowance or interest resulting from payments made by the federal Medicaid program as reimbursement for claims providing TCM services pursuant to Welfare and Institutions Code section 14132.44, for the disallowed claim or claims, less the amounts already remitted to DHCS pursuant to Welfare and Institutions Code section 14132.44(m).

B. To the extent that a federal audit disallowance and interest results from a claim or claims for which the Provider has received reimbursement for TCM services, DHCS shall recoup from the Provider, upon 60 days written notice, amounts equal to the amount of the disallowance and interest in that SFY for the disallowed claim or claims. All subsequent TCM Summary Invoices submitted to DHCS applicable to any previously disallowed claim or claims, may be held in abeyance, with no payment made, until the federal disallowance issue is resolved, less the amounts already remitted to DHCS pursuant to Welfare and Institutions Code section 14132.44, subdivision (m).

C. Notwithstanding Article 2 and Article 7, to the extent that a federal audit disallowance or interest results from a claim or claims for which the Provider has received reimbursement for TCM services provided by a non-governmental entity under contract with, and on behalf of the Provider, DHCS shall be held harmless by the Provider for 100 percent of the amount of any such federal audit disallowance and interest, for the disallowed claim or claims, less the amounts already remitted to DHCS pursuant to Welfare and Institutions Code section 14132.44, subdivision (m).

D. Notwithstanding Article 2 and Article 7, the Provider agrees that when it is established upon audit or reconciliation that an overpayment, or other recovery determination, has been made, DHCS and Provider shall follow current laws, regulations, and state issued policy directives, including PPLs for the proper treatment of identified overpayment.

E. DHCS reserves the right to select the method to be used for the recovery of an overpayment, or other recovery determination.

F. Overpayments may be assessed interest charges, and may be assessed penalties, in accordance with Welfare and Institutions Code sections 14171, subdivision (h), and 14171.5, respectively.

ARTICLE IX – AMENDMENT

Should either party, during the term of this PPA desire an amendment to the Articles of this PPA, such changes or amendments shall be proposed in writing to the other party, who will respond in writing as to whether the proposed amendments are accepted or

rejected. If accepted and after negotiations are concluded, the agreed upon changes shall be made through a process that is mutually agreeable to both DHCS and the Provider. No amendment is binding on either party until it is approved by DHCS.

ARTICLE X – CONFLICT OF INTEREST

DHCS intends to avoid any real or apparent conflict of interests on the part of the Provider, subcontractors, employees, officers or directors of the Provider or subcontractors. DHCS reserves the right to determine at its sole discretion, whether any information, assertion, or claim received from any source indicates the existence of a real or apparent conflict of interest. If a conflict exists, DHCS has the authority to require the LGA to submit additional information or a plan for resolving the conflict, subject to DHCS' review and prior approval.

A. Conflicts of interest include but are not limited to:

   1. An instance where the Provider, its subcontractors, or any employee, officer, or director of the Provider or subcontractor has an interest, financial or otherwise, where the use or disclosure of any information obtained while performing services under the contract would allow for private or personal benefit or for any purpose that is contrary to the goals and objectives of the PPA.

   2. An instance where the Provider's or any subcontractor's employees, officers, or directors use their positions for purposes that are or give the appearance of being, motivated by a desire for private gain for either themselves, or those with whom they have familial, business, or other ties.

If DHCS becomes aware of a known or suspected conflict of interest, the Provider will have an opportunity to submit additional information or resolve the conflict. A Provider with a suspected conflict of interest will have five working days from the date of notification of the conflict by DHCS to provide complete information regarding the suspected conflict. DHCS shall have the right to terminate the PPA, if DHCS determines that that a conflict of interest exists, and the conflict cannot be resolved to the satisfaction of DHCS. DHCS, at its discretion, may authorize an extension of the timeline for providing additional documentation indicated herein upon receiving written receipt from the Provider.

ARTICLE XI – GENERAL PROVISIONS

A. This document, including any attachments or exhibits, constitutes the entire PPA between the parties pertaining to the TCM Program. Notwithstanding DHCS Form 6207 and DHCS Form 6208, any condition, provision, agreement or understanding not stated in this PPA shall not affect any rights, duties, or privileges in connection with the terms of this PPA. If there is a conflict between this PPA and DHCS Form 6207 and DHCS Form 6208, then DHCS Form 6207 and DHCS Form 6208 shall control. DHCS Form 6207 and DHCS Form 6208 are hereby incorporated by reference and are made part of this PPA.

B. The term "days" as used in this PPA shall mean calendar days unless otherwise specified.

C. The provisions and obligations of this PPA cannot be waived or altered except through an amendment made in accordance with Article IX.

D. None of the provisions of this PPA are or shall be construed as for the benefit of, or enforceable by, any person not a party to this PPA.

<Signature page to follow>

###

TCM AGREEMENT EXECUTION

The undersigned agent agrees to the terms above, and enters into this PPA on behalf of City of Long Beach (Provider).

Provider Authorized Contact Person's Signature

Patrick H. West
Print Name

City Manager
Title

Tom Modica
~~Assistant~~ City Manager
EXECUTED PURSUANT TO SECTION 301 OF ~~THE CITY~~ CHARTER

333 West Ocean Blvd., Long Beach, CA 90802
Address

2/27/19
Date

California Department of Health Care Services
Authorized Contact Person's Signature

John Mendoza
Print Name

Chief, Safety Net Financing Division
Title

Department of Health Care Services
Name of Department

1501 Capitol Avenue, MS 4603, Sacramento, CA 95899-7413
Address

5/13/19
Date

APPROVED AS TO FORM
Feb. 20, 20 19
CHARLES PARKIN, City Attorney
By
GARY J. ANDERSON
PRINCIPAL DEPUTY CITY ATTORNEY

Exhibit A
HIPAA Business Associate Addendum

I. Recitals

A. This Contract (Agreement) has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ('the HITECH Act"), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").

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

C. As set forth in this Agreement, Contractor, here and after, is the Business Associate of DHCS acting on DHCS' behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of DHCS and creates, receives, maintains, transmits, uses or discloses PHI and PI. DHCS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties."

D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that DHCS must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act, and the Final Omnibus Rule as well as the Alcohol and Drug Abuse patient records confidentiality law 42 CFR Part 2, and any other applicable state or federal law or regulation. 42 CFR section 2.1(b)(2)(B) allows for the disclosure of such records to qualified personnel for the purpose of conducting management or financial audits, or program evaluation. 42 CFR Section 2.53(d) provides that patient identifying information disclosed under this section may be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by an appropriate court order.

E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

II. Definitions

A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the Final Omnibus Rule.

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

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

D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.

Exhibit A
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

Exhibit A
HIPAA Business Associate Addendum

HIPAA regulations, if done by DHCS. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, the HIPAA regulations, the Final Omnibus Rule and 42 CFR Part 2.

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

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

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

B. Prohibited Uses and Disclosures

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).

2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of DHCS and as permitted by 42 U.S.C. section 17935(d)(2).

C. Responsibilities of Business Associate

Business Associate agrees:

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

2. ***Safeguards.*** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of DHCS, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities, and

Exhibit A
HIPAA Business Associate Addendum

which incorporates the requirements of section 3, Security, below. Business Associate will provide DHCS with its current and updated policies.

3. ***Security.*** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

   a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;

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

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

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

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

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

E. ***Business Associate's Agents and Subcontractors.***

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

Exhibit A
HIPAA Business Associate Addendum

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

   a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by DHCS; or

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

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

1. To provide access as DHCS may require, and in the time and manner designated by DHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to DHCS (or, as directed by DHCS), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for DHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DHCS health plans; or those records used to make decisions about individuals on behalf of DHCS. Business Associate shall use the forms and processes developed by DHCS for this purpose and shall respond to requests for access to records transmitted by DHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable DHCS to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).

3. If Business Associate receives data from DHCS that was provided to DHCS by the Social Security Administration, upon request by DHCS, Business Associate shall provide DHCS with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

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

H. ***Internal Practices.*** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from DHCS, or created or received by Business Associate on behalf of DHCS, available to DHCS or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by DHCS or by the Secretary, for purposes of determining DHCS' compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to DHCS and shall set forth the efforts it made to obtain the information.

Exhibit A
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 A
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 A
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 A
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.

Exhibit A
HIPAA Business Associate Addendum

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

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

VII. Miscellaneous Provisions

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

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

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

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

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

Exhibit A
HIPAA Business Associate Addendum

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

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

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

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

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

Exhibit A
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.

Exhibit A
HIPAA Business Associate Addendum

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

F. ***Patch Management.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

G. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DHCS PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

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

H. ***Data Destruction.*** When no longer needed, all DHCS PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.

I. ***System Timeout.*** The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

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

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

L. ***Access Controls.*** The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

Exhibit A
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.

Exhibit A
HIPAA Business Associate Addendum

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

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

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

F. ***Mailing.*** Mailings of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.

DEPARTMENT OF HEALTH CARE SERVICES

HIPAA Business Associate Addendum

Attachment A

The following data files will be provided pursuant to this Agreement:

Managed Care Organization (MCO)

Each MCO will receive a list of Medi-Cal Participants (Participant) who received TCM services that is/was enrolled in that MCO. The list may provide the following information, as necessary, for each Participant who received TCM services:

1. Last Name
2. First Name
3. Middle Name
4. Date Of Birth
5. Sex
6. MEDS ID
7. LGA Name (Most recent LGA that provided care)
8. Program Type
9. Encounter Number
10. Date Of Service
11. California ID Number

Local Government Agency (LGA)

Each LGA will receive a list of Participants who received TCM services from the LGA. The list may provide the following information, as necessary, for each Participant who received TCM services:

1. Last Name
2. First Name
3. Middle Name
4. Date Of Birth
5. Sex
6. MEDS ID
7. LGA Name
8. Program Type
9. Encounter Number
10. Date Of Service
11. MCO Name (Most recent MCO that Participant is/was enrolled in)
12. California ID Number