

Exhibit E
Additional Provisions

1. Amendment Process

Should either party, during the term of this Agreement, desire a change or amendment to the terms of this Agreement, such changes or amendments shall be proposed in writing to the other party, who will respond in writing as to whether the proposed changes/amendments are accepted or rejected. If accepted and after negotiations are concluded, the agreed upon changes shall be made through the State's official agreement amendment process. No amendment will be considered binding on either party until it is formally approved by the both parties and the Department of General Services (DGS), if DGS approval is required.

2. Cancellation/Termination

A. General Provisions

- 1) As required by Welf. & Inst. Code § 14712, if the Contractor decides not to contract with the Department, does not renew its contract, or is unable to meet the standards set by the Department, the Contractor agrees to inform the Department of this decision in writing.
- 2) If the Contractor is unwilling to contract for the delivery of specialty mental health services or if the Department or Contractor determines that the Contractor is unable to adequately provide specialty mental health services or that the Contractor does not meet the standards the Department deems necessary for a mental health plan, the Department shall ensure that specialty mental health services are provided to Medi-Cal beneficiaries.
- 3) The Department may contract with qualifying individual counties, counties acting jointly, or other qualified entities approved by the Department for the delivery of specialty mental health services in any county that is unable or unwilling to contract with the Department. The Contractor may not subsequently contract to provide specialty mental health services unless the Department elects to contract with the Contractor.
- 4) If the Contractor does not contract with the Department to provide specialty mental health services, the Department will work with the Department of Finance and the Controller to obtain funds from the Contractor in accordance with Government (Govt.) Code 30027.10.

B. Contract Renewal

- 1) Pursuant to Welf. & Inst. Code § 14714(b), this contract may be renewed if the Contractor continues to meet the statutory and regulatory requirements governing this contract, as well as the terms and conditions of this contract. Failure to meet these requirements shall be cause for nonrenewal of the contract. The Department may base the decision to renew on timely

Exhibit E
Additional Provisions

completion of a mutually agreed-upon plan of correction of any deficiencies, submissions of required information in a timely manner, and/or other conditions of the contract.

- 2) In the event the contract is not renewed based on the reasons specified in (1), the Department will notify the Department of Finance, the fiscal and policy committees of the Legislature, and the Controller of the amounts to be sequestered from the Mental Health Subaccount, the Mental Health Equity Account, and the Vehicle License Fee Collection Account of the Local Revenue Fund and the Mental Health Account and the Behavioral Health Subaccount of the Local Revenue Fund 2011, and the Controller will sequester those funds in the Behavioral Health Subaccount pursuant to Govt. Code § 30027.10. Upon this sequestration, the Department will use the funds in accordance with Govt. Code § 30027.10

C. Contract Amendment Negotiations

Should either party during the life of this contract desire a change in this contract, such change shall be proposed in writing to the other party. The other party shall acknowledge receipt of the proposal in writing within 10 days and shall have 60 days (or such different period as the parties mutually may set) after receipt of such proposal to review and consider the proposal, to consult and negotiate with the proposing party, and to accept or reject the proposal. Acceptance or rejection may be made orally within the 60-day period, and shall be confirmed in writing within five days thereafter. The party proposing any such change shall have the right to withdraw the proposal at any time prior to acceptance or rejection by the other party. Any such proposal shall set forth a detailed explanation of the reason and basis for the proposed change, a complete statement of costs and benefits of the proposed change and the text of the desired amendment to this contract that would provide for the change. If the proposal is accepted, this contract shall be amended to provide for the change mutually agreed to by the parties on the condition that the amendment is approved by the Department of General Services, if necessary.

D. Contract Termination

The Department or the Contractor may terminate this contract in accordance with Cal. Code Regs., tit. 9, § 1810.323.

- 1) DHCS reserves the right to cancel or terminate this Agreement immediately for cause.
- 2) The term "for cause" shall mean that the Contractor fails to meet the terms, conditions, and/or responsibilities of this Agreement.

Exhibit E
Additional Provisions

- 3) Agreement termination or cancellation shall be effective as of the date indicated in DHCS' notification to the Contractor. The notice shall identify any final performance, invoicing or payment requirements.
- 4) Upon receipt of a notice of termination or cancellation, the Contractor shall take immediate steps to stop performance and to cancel, or if cancelation is not possible reduce, subsequent agreement costs.
- 5) In the event of early termination or cancellation, the Contractor shall be entitled to payment for all allowable costs authorized under this Agreement and incurred up to the date of termination or cancellation, including authorized non-cancelable obligations, provided such expenses do not exceed the stated maximum amounts payable.
- 6) Pursuant to the Welf. & Inst. Code § 14714(d), the Department will immediately terminate a contract when the director finds that there is an immediate threat to the health and safety of Medi-Cal beneficiaries. Termination of the contract for other reasons will be subject to reasonable notice to the Contractor of the Department's intent to terminate, as well as notification to affected beneficiaries.

E. Termination of Obligations

- 1) All obligations to provide covered services under this contract shall automatically terminate on the effective date of any termination of this contract. The Contractor shall be responsible for providing covered services to beneficiaries until the termination or expiration of the contract and shall remain liable for the processing and payment of invoices and statements for covered services provided to beneficiaries prior to such expiration or termination.
- 2) When Contractor terminates a subcontract with a provider, Contractor shall make a good faith effort to provide notice of this termination, within 15 days, to the persons that Contractor, based on available information, determines have recently been receiving services from that provider.

F. Contract Disputes

Should a dispute arise between the Contractor and the Department relating to performance under this contract, other than disputes governed by a dispute resolution process in Chapter 11 of Division 1, Cal. Code Regs., tit. 9, or the processes governing the audit appeals process in Chapter 9 of Division 1, Cal. Code Regs., tit. 9 the Contractor shall follow the Dispute Resolution Process outlined in provision number 15 of Exhibit D(F) which is attached hereto as part of this agreement.

Exhibit E
Additional Provisions

3. Fulfillment of Obligation

No covenant, condition, duty, obligation, or undertaking continued or made a part of this contract shall be waived except by written agreement of the parties hereto, and forbearance or indulgence in any other form or manner by either party in any regard whatsoever will not constitute a waiver of the covenant, condition, duty, obligation, or undertaking to be kept, performed or discharged by the party to which the same may apply. Until performance or satisfaction of all covenants, conditions, duties, obligations, and undertakings is complete, the other party shall have the right to invoke any remedy available under this contract, or under law, notwithstanding such forbearance or indulgence.

4. Additional Provisions

A. Inspection Rights

The Contractor shall allow the Department, DHCS, HHS, the Comptroller General of the United States, and other authorized federal and state agencies, or their duly authorized representatives, to inspect or otherwise evaluate the quality, appropriateness, and timeliness of services performed under this contract, and to inspect, evaluate, and audit any and all books, records, and facilities maintained by the Contractor and its subcontractors pertaining to such services at any time during normal business hours. Books and records include, but are not limited to, all physical records originated or prepared pursuant to the performance under this contract including working papers, reports, financial records and books of account, beneficiary records, prescription files, subcontracts, and any other documentation pertaining to covered services and other related services for beneficiaries. Upon request, at any time during the period of this contract, the Contractor shall furnish any such record, or copy thereof, to the Department, DHCS, or HHS. Authorized agencies shall maintain the confidentiality of such books and records in accordance with applicable laws and regulations.

B. Notices

Unless otherwise specified in this contract, all notices to be given under this contract shall be in writing and shall be deemed to have been given when mailed, to the Department or the Contractor at the following addresses, unless the contract explicitly requires notice to another individual or organizational unit:

Department of Health Care Services
Mental Health Services Division
1500 Capitol Avenue, MS 2702
P.O. Box 997413
Sacramento, CA 95899-7413

El Dorado County Health and Human
Services Agency
3057 Briw Road, Suite A
Placerville, CA 95667

C. Nondiscrimination

Exhibit E
Additional Provisions

- 1) Consistent with the requirements of applicable federal law such as 42 C.F.R. §§ 438.6(d)(3) and (4) or state law, the Contractor shall not engage in any unlawful discriminatory practices in the admission of beneficiaries, assignments of accommodations, treatment, evaluation, employment of personnel, or in any other respect on the basis of race, color, gender, religion, marital status, national origin, age, sexual preference or mental or physical handicap. The Contractor will not discriminate against beneficiaries on the basis of health status or need for health care services, pursuant to 42 C.F.R. § 438.6(d)(3).
- 2) The Contractor shall comply with the provisions of Section 504 of the Rehabilitation Act of 1973, as amended, pertaining to the prohibition of discrimination against qualified handicapped persons in all federally assisted programs or activities, as detailed in regulations signed by the Secretary of Health and Human Services, effective June 2, 1977, and found in the Federal Register, Volume 42, No. 86, dated May 4, 1977.
- 3) The Contractor shall include the nondiscrimination and compliance provisions of this contract in all subcontracts to perform work under this contract.
- 4) Notwithstanding other provisions of this section, the Contractor may require a determination of medical necessity pursuant to Cal. Code Regs., tit. 9, §§ 1820.205, 1830.205 and/or 1830.210, prior to providing covered services to a beneficiary.

D. Patients' Rights

- 1) The parties to this contract shall comply with applicable laws and regulations relating to patients' rights, including but not limited to Welfare and Institutions Code 5325, Cal. Code Regs., tit. 9, §§ 860 through 868, and 42 C.F.R. § 438.100. The Contractor shall ensure that its subcontractors comply with these provisions.
- 2) Pursuant to 42 C.F.R. § 438.100, the Contractor shall have written policies regarding the beneficiary rights specified in this section and ensure that its staff and subcontract providers take those rights into account when providing services, including the right to:
 - a) Receive information in accordance with 42 C.F.R. § 438.10.
 - b) Be treated with respect and with due consideration for his or her dignity and privacy.
 - c) Receive information on available treatment options and alternatives, presented in a manner appropriate to the beneficiary's condition and ability to understand.

Exhibit E
Additional Provisions

- d) Participate in decisions regarding his or her health care, including the right to refuse treatment.
- e) Be free from any form of restraint or seclusion used as a means of coercion, discipline, convenience, or retaliation.
- f) Request and receive a copy of his or her medical records, and to request that they be amended or corrected, as specified in 45 C.F.R. §§ 164.524 and 164.526.
- g) To be furnished services in accordance with 42 C.F.R. §§ 438.206 through 438.210.
- h) To freely exercise his or her rights, and the exercise of those rights will not adversely affect the way the Contractor and its providers or the Department treat the beneficiary.

E. Relationship of the Parties

The Department and the Contractor are, and shall at all times be deemed to be, independent agencies. Each party to this contract shall be wholly responsible for the manner in which it performs the obligations and services required of it by the terms of this contract. Nothing herein contained shall be construed as creating the relationship of employer and employee, or principal and agent, between the parties or any of their agents or employees. Each party assumes exclusively the responsibility for the acts of its employees or agents as they relate to the services to be provided during the course and scope of their employment. The Department and its agents and employees shall not be entitled to any rights or privileges of the Contractor's employees and shall not be considered in any manner to be Contractor employees. The Contractor and its agents and employees, shall not be entitled to any rights or privileges of state employees and shall not be considered in any manner to be state employees.

F. Waiver of Default

Waiver of any default shall not be deemed to be a waiver of any subsequent default. Waiver of breach of any provision of this agreement shall not be deemed to be a waiver of any other or subsequent breach, and shall not be construed to be a modification of the terms of this contract.

5. Duties of the State

In discharging its obligations under this contract, and in addition to the obligations set forth in other parts of this contract, the Department shall perform the following duties:

A. Payment for Services

Exhibit E
Additional Provisions

The Department shall make the appropriate payments set forth in Exhibit B and take all available steps to secure and pay FFP to the Contractor, once the Department receives FFP, for claims submitted by the Contractor. The Department shall notify Contractor and allow Contractor an opportunity to comment to the Department when questions are posed by CMS, or when there is a federal deferral, withholding, or disallowance with respect to claims made by the Contractor.

B. Reviews

The Department shall conduct reviews of access to and quality of care in Contractor's county at least once every three years and issue reports to the Contractor detailing findings, recommendations, and corrective action, as appropriate, pursuant to Cal. Code Regs., tit. 9, §§ 1810.380 and 1810.385. The Department shall also arrange for an annual external quality review of the Contractor as required by 42 C.F.R. § 438.204(d) and Cal. Code Regs., tit. 9, § 1810.380(a)(7).

C. Monitoring for Compliance

The Department shall monitor the Contractor's operations for compliance with the provisions of this contract, and applicable federal and state law and regulations. Such monitoring activities shall include, but not be limited to, inspection and auditing of Contractor facilities, management systems and procedures, and books and records, as the Department deems appropriate, at any time during the Contractor's or facility's normal business hours. When monitoring activities identify areas of non-compliance, the Department shall issue reports to the Contractor detailing findings, recommendations, and corrective action. Failure to comply with required corrective action could lead to civil penalties, as appropriate, pursuant to Cal. Code Regs., tit. 9, §§ 1810.380 and 1810.385.

D. The Department shall review and either approve, disapprove, or request additional information for each Implementation Plan as defined in Cal. Code Regs., tit. 9, §§ 1810.221 and 1810.310 . Notices of Approval, Notices of Disapproval and requests for additional information shall be forwarded to the Contractor within 60 days of the receipt of the Implementation Plan. A Contractor shall submit proposed changes to its approved Implementation Plan in writing to the Department for review. A Contractor shall submit proposed changes in the policies, processes or procedures that would modify the Contractor's current Implementation Plan prior to implementing the proposed changes.(See Cal. Code Regs., tit. 9, § 1810.310 (b)-(c)).

E. The Department shall act promptly to review the Contractor's Cultural Competence Plan submitted pursuant to Cal. Code Regs., tit. 9, § 1810.410. The Department shall provide a Notice of Approval or a Notice of Disapproval, including the reasons for the disapproval, to the Contractor within 60 calendar days after receipt of the

Exhibit E
Additional Provisions

plan from the Contractor. If the Department fails to provide a Notice of Approval or Disapproval, the Contractor may implement the plan 60 calendar days from its submission to the Department.

F. Certification of Organizational Provider Sites Owned or Operated by the Contractor

- 1) The Department shall certify the organizational provider sites that are owned, leased or operated by the Contractor, in accordance with Cal. Code Regs., tit. 9, § 1810.435, and the requirements specified in Exhibit B, Section 4 of this contract. This certification shall be performed prior to the date on which the Contractor begins to deliver services under this contract at these sites and once every three years after that date, unless the Department determines an earlier date is necessary. The on-site review required by Cal. Code Regs., tit. 9, § 1810.435(e), shall be conducted of any site owned, leased, or operated by the Contractor and used for to deliver covered services to beneficiaries, except that on-site review is not required for public school or satellite sites.
- 2) The Department may allow the Contractor to begin delivering covered services to beneficiaries at a site subject to on-site review by the Department prior to the date of the on-site review, provided the site is operational and has any required fire clearances. The earliest date the Contractor may begin delivering covered services at a site subject to on site review by the Department is the date the Contractor requested certification of the site in accordance with procedures established by the Department, the date the site was operational, or the date a required fire clearance was obtained, whichever date is latest.
- 3) The Department may allow the Contractor to continue delivering covered services to beneficiaries at a site subject to on-site review by the Department as part of the recertification process prior to the date of the on-site review, provided the site is operational and has all required fire clearances.
- 4) Nothing in this section precludes the Department from establishing procedures for issuance of separate provider identification numbers for each of the organizational provider sites operated by the Contractor to facilitate the claiming of FFP by the Contractor and the Department's tracking of that information.

G. Distribution of Informing Materials

The Department shall provide annual notice to all beneficiaries in accordance with 42 C.F.R. § 438.10(f)(2), and Cal. Code Regs., tit. 9, § 1810.360(c).

H. Sanctions

Exhibit E
Additional Provisions

The Department shall conduct oversight and impose sanctions on the Contactor for violations of the terms of this contract, and applicable federal and state law and regulations, in accordance with Welf. & Inst. Code § 14712(e) and Cal. Code Regs., tit. 9, §§ 1810.380 and 1810.385.

I. Notification

The Department shall notify beneficiaries of their Medi-Cal specialty mental health benefits and options available upon termination or expiration of this contract.

J. Performance Measurement

The Department shall measure the Contractor's performance based on Medi-Cal approved claims and other data available to the Department using standard measures established by the Department in consultation with stakeholders.

6. State and Federal Law Governing this Contract

- A. Contractor agrees to comply with all applicable federal and state law, including the applicable sections of the state plan and waiver, particularly the statutes and regulations incorporated by reference below, in its provision of services as the Mental Health Plan. The Department will notify Contractor of any changes to these statutes and regulations. Contractor agrees to comply with any changes to these statutes and regulations that may occur during the contract period and any new applicable statutes or regulations, but either the Department or Contractor may request consultation and discussion of new or changed statutes or regulations, including whether contract amendments may be necessary.
- B. Pursuant to Welf. & Inst. Code § 14704, a regulation or order concerning Medi-Cal specialty mental health services adopted by the State Department of Mental Health pursuant to Division 5 (commencing with Section 5000), as in effect preceding the effective date of this section, shall remain in effect and shall be fully enforceable, unless and until the readoption, amendment, or repeal of the regulation or order by DHCS, or until it expires by its own terms.
- C. Specifically, the following federal law applies to this contract:
- 1) Title 42 United States Code, to the extent that these requirements are applicable
 - 2) 42 C.F.R. to the extent that these requirements are applicable;
 - 3) 42 C.F.R. § 438 – Managed Care, limited to those provisions that apply to Prepaid Inpatient Health Plans (PIHP);
 - 4) 45 C.F.R. §§ 160 and 164 to the extent that these requirements are applicable;

Exhibit E
Additional Provisions

- 5) Title VI of the Civil Rights Act of 1964;
- 6) Title IX of the Education Amendments of 1972;
- 7) Age Discrimination Act of 1975;
- 8) Rehabilitation Act of 1973;
- 9) Titles II and III of the Americans with Disabilities Act;
- 10) Deficit Reduction Act of 2005;
- 11) Balanced Budget Act of 1997.
- 12) The Contractor shall comply with the provisions of the Copeland Anti-Kickback Act, which requires that all contracts and subcontracts in excess of \$2000 for construction or repair awarded by the Contractor and its subcontractors shall include a provision for compliance with the Copeland Anti-Kickback Act.
- 13) The Contractor shall comply with the provisions of the Davis-Bacon Act, as amended, which provides that, when required by Federal Medicaid program legislation, all construction contracts awarded by the Contractor and its subcontractors of more than \$2,000 shall include a provision for compliance with the Davis-Bacon Act as supplemented by Department of Labor regulations.
- 14) The Contractor shall comply with the provisions of the Contract Work Hours and Safety Standards Act, as applicable, which requires that all subcontracts awarded by the Contractor in excess of \$2,000 for construction and in excess of \$2,500 for other subcontracts that involve the employment of mechanics or laborers shall include a provision for compliance with the Contract Work Hours and Safety Standards Act.

D. State Law:

- 1) Division 5, Welf. & Inst. Code, to the extent that these requirements are applicable to the services and functions set forth in this contract
- 2) Welf. & Inst. Code §§ 5779-5782
- 3) Welf. & Inst. Code §§ 14680-14685.1
- 4) Welf. & Inst. Code §§ 14700-14726

Exhibit E
Additional Provisions

- 5) Chapter 7, Division 9, Welf. & Inst. Code, to the extent that these requirements are applicable to the services and functions set forth in this contract
- 6) Cal. Code Regs., tit. 9, § 1810.100 et. seq. – Medi-Cal Specialty Mental Health Services
- 7) Cal. Code Regs., tit. 22, §§ 50951 and 50953
- 8) Cal. Code Regs., tit. 22, §§ 51014.1 and 51014.2

EXHIBIT F

Privacy and Information Security Provisions

Exhibit F is intended to protect the privacy and security of specified Department information that Contractor may access, receive, or transmit under this Agreement. The Department information covered under this Exhibit F consists of: (1) Protected Health Information (PHI) as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA")(PHI); and (2) Personal Information (PI) as defined under the California Information Practices Act (CIPA), at California Civil Code § 1798.3. Personal Information may include data provided to the Department by the Social Security Administration.

Exhibit F consists of the following parts:

- A. Part I, HIPAA Business Associate Addendum, which provides for the privacy and security of PHI.
- B. Part II, which provides for the privacy and security of PI in accordance with specified provisions of the IEA and the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (Computer Agreement) to the extent Contractor access, receives, or transmits PI under these Agreements. Exhibit F, Part II, further provides for the privacy and security of PI as defined under Civil Code §§ 1798.3(a) and 1798.29. These terms of the California Information Practices Act (CIPA) are included here because they do not apply to counties directly, and the statute requires the Department to contractually extend these CIPA terms to contractors if they use the Department's PI to accomplish a function for the Department.
- C. Part III, Miscellaneous Provision, sets forth additional terms and conditions that extend to the provisions of Exhibit F in its entirety.

EXHIBIT F
Privacy and Information Security Provisions

Part I: HIPAA Business Associate Addendum

1. Recitals

- A. 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. § 17921 et seq., and their implementing privacy and security regulations at 45 C.F.R. Parts 160 and 164 ("the HIPAA regulations") between Department and Contractor arises only to the extent that Contractor performs functions or activities on behalf of the Department pursuant to this Agreement that are described in the definition of "business associate" in 45 C.F.R. § 160.103, including but not limited to utilization review, quality assurance, or benefit management.
- B. The Department wishes to disclose to Contractor 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, to be used or disclosed in the course of providing services and activities as set forth in Section 1.A. of Exhibit F, Part I of this Agreement. This information is hereafter referred to as "Department PHI".
- C. To the extent Contractor performs the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit F, Part I of this Agreement, Contractor is the Business Associate of the Department acting on the Department's behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of the Department and creates, receives, maintains, transmits, uses or discloses PHI and ePHI in the provision of such services or in the performance of such functions or activities. The Department and Contractor are each a party to this Agreement and are collectively referred to as the "parties."
- D. The purpose of this Part I is to protect the privacy and security of the PHI and ePHI 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 the Department must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 C.F.R. Parts 160 and 164 and the HITECH Act.
- E. The terms used in this Part I, 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.

EXHIBIT F

Privacy and Information Security Provisions

2. Definitions

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- D. Department PHI shall mean Protected Health Information or Electronic Protected Health Information, as defined below, accessed by Contractor in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services on behalf of the Department as specified in Section 1.A. of Exhibit F, Part I of this Agreement. The terms PHI as used in this document shall mean Department PHI.
- E. Electronic Health Records shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. § 17921 and implementing regulations.
- F. 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 C.F.R. § 160.103.
- G. 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 C.F.R. § 160.103.
- H. Privacy Rule shall mean the HIPAA Regulations that are found at 45 C.F.R. Parts 160 and 164, Subparts A and E.
- I. Protected Health Information (PHI) 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 C.F.R. § 160.103 and as defined under HIPAA.

EXHIBIT F**Privacy and Information Security Provisions**

- J. Required by law, as set forth under 45 C.F.R. § 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 Department PHI, or confidential data utilized by Contractor to perform the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit F, Part I of this Agreement; or interference with system operations in an information system that processes, maintains or stores Department PHI.
- M. Security Rule shall mean the HIPAA regulations that are found at 45 C.F.R. Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. § 17932(h), any guidance issued by the Secretary pursuant to such Act and the HIPAA regulations.

3. Terms of Agreement

- A. **Permitted Uses and Disclosures of Department PHI by Contractor.** Except as otherwise indicated in this Exhibit F, Part I, Contractor may use or disclose Department PHI only to perform functions, activities or services specified in Section 1.A of Exhibit F, Part I of this Agreement, for, or on behalf of the Department, provided that such use or disclosure would not violate the HIPAA regulations, if done by the Department. Any such use or disclosure, if not for purposes of treatment activities of a health care provider as defined by the Privacy Rule, must, to the extent practicable, be limited to the limited data set, as defined in 45 C.F.R. § 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.
- B. **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Exhibit F, Part I, Contractor may:

EXHIBIT F**Privacy and Information Security Provisions**

- 1) **Use and disclose for management and administration.** Use and disclose Department PHI for the proper management and administration of the Contractor's business, provided that such disclosures are required by law, or the Contractor 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 Contractor of any instances of which it is aware that the confidentiality of the information has been breached.
- 2) **Provision of Data Aggregation Services.** Use Department PHI to provide data aggregation services to the Department to the extent requested by the Department and agreed to by Contractor. Data aggregation means the combining of PHI created or received by the Contractor, as the Business Associate, on behalf of the Department 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 the Department.

C. Prohibited Uses and Disclosures

- 1) Contractor shall not disclose Department PHI about an individual to a health plan for payment or health care operations purposes if the Department 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. §§ 17935(a) and 45 C.F.R. § 164.522(a).
- 2) Contractor shall not directly or indirectly receive remuneration in exchange for Department PHI, except with the prior written consent of the Department and as permitted by 42 U.S.C. § 17935(d)(2).

D. Responsibilities of Contractor

Contractor agrees:

- 1) **Nondisclosure.** Not to use or disclose Department PHI other than as permitted or required by this Agreement or as required by law.
- 2) **Compliance with the HIPAA Security Rule.** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Department PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of the Department, in compliance with 45 C.F.R. §§ 164.308, 164.310 and 164.312, and to prevent use or disclosure of Department PHI other than as provided for by this Agreement. Contractor shall implement reasonable and appropriate policies and procedures to comply with the standards,

EXHIBIT F**Privacy and Information Security Provisions**

implementation specifications and other requirements of 45 C.F.R. § 164, subpart C, in compliance with 45 C.F.R. § 164.316. Contractor 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 Contractor's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Contractor will provide the Department with its current and updated policies upon request.

- 3) **Security.** Contractor shall 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, Business Associate Data Security Requirements;
 - b) Achieving and maintaining compliance with the HIPAA Security Rule (45 C.F.R. Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement; and
 - 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.
- 4) **Security Officer.** Contractor 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 the Department.
- 5) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PHI by Contractor or its subcontractors in violation of the requirements of this Exhibit F, Part I.
- 6) **Reporting Unauthorized Use or Disclosure.** To report to Department any use or disclosure of Department PHI not provided for by this Exhibit F, Part I of which it becomes aware.
- 7) **Contractor's Agents and Subcontractors.**
 - a) To enter into written agreements with any agents, including subcontractors and vendors to whom Contractor provides Department PHI, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Contractor

EXHIBIT F**Privacy and Information Security Provisions**

with respect to such Department PHI under this Exhibit F, and that require compliance with all applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI. Contractor shall incorporate, when applicable, the relevant provisions of this Exhibit F, Part I into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI be reported to Contractor.

- b) In accordance with 45 C.F.R. § 164.504(e)(1)(ii), upon Contractor's knowledge of a material breach or violation by its subcontractor of the agreement between Contractor and the subcontractor, Contractor shall:
 - i. 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 the Department; or
 - ii. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

8) Availability of Information to the Department and Individuals to Provide Access and Information:

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

EXHIBIT F**Privacy and Information Security Provisions**

- b) If Contractor maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Contractor shall provide such information in an electronic format to enable the Department to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. § 17935(e). This section shall be effective as of the date that 42 U.S.C. § 17935(e) and its implementing regulations apply to the Department.
- 9) **Amendment of Department PHI.** To make any amendment(s) to Department PHI that were requested by a patient and that the Department directs or agrees should be made to assure compliance with 45 C.F.R. § 164.526, in the time and manner designated by the Department, with the Contractor being given a minimum of twenty (20) days within which to make the amendment.
- 10) **Internal Practices.** To make Contractor's internal practices, books and records relating to the use and disclosure of Department PHI available to the Department or to the Secretary, for purposes of determining the Department's 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 Contractor, Contractor shall provide written notification to the Department and shall set forth the efforts it made to obtain the information.
- 11) **Documentation of Disclosures.** To document and make available to the Department or (at the direction of the Department) to an Individual such disclosures of Department PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of such PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 C.F.R. § 164.528 and 42 U.S.C. § 17935(c). If Contractor maintains electronic health records for the Department as of January 1, 2009, Contractor 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 Contractor acquires electronic health records for the Department after January 1, 2009, Contractor 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. This section shall be effective only as of the date that 42 U.S.C. § 17935(c) and its implementing regulations apply to the Department.
- 12) **Breaches and Security Incidents.** During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and

EXHIBIT F**Privacy and Information Security Provisions**

prompt reporting of any breach or security incident, and to take the following steps:

- a) **Initial Notice to the Department.** (1) To notify the Department **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured PHI in electronic media or in any other media if the PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. (2) To notify the Department **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement or this Exhibit F, Part I, 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.
- b) Notice shall be provided to the Department Program Contract Manager and the Department Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the Department Information Security Officer. Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link:

<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx>
- c) Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI , Contractor shall take:
 - i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
 - ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- d) **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI . Within 72 hours of

EXHIBIT F**Privacy and Information Security Provisions**

the discovery, Contractor shall submit an updated "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 Department Program Contract Manager and the Department Information Security Officer.

- e) **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Department Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "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, and the HIPAA regulations. 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 the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten(10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. 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 "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.
- f) **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in 42 U.S.C. § 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured Department PHI involves more than 500 residents of the State of California or its jurisdiction, Contractor shall notify the Secretary of the breach immediately upon discovery of the breach. If Contractor 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 the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

EXHIBIT F

Privacy and Information Security Provisions

- g) **Responsibility for Notification of Affected Individuals.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors and notification of the affected individuals is required under state or federal law, Contractor shall bear all costs of such notifications as well as any costs associated with the breach. In addition, the Department reserves the right to require Contractor to notify such affected individuals, which notifications shall comply with the requirements set forth in 42 U.S.C. § 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 Department Program Contract Manager and the Department 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. The Department will provide its review and approval expeditiously and without unreasonable delay.

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

Department Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
See the Exhibit A, Scope of Work 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	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Service Desk (916) 440-7000 or (800)

- 13) **Termination of Agreement.** In accordance with § 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Contractor knows of a material breach or violation by the Department of this Exhibit F, Part I, it shall take the following steps:

EXHIBIT F**Privacy and Information Security Provisions**

- a) Provide an opportunity for the Department to cure the breach or end the violation and terminate the Agreement if the Department does not cure the breach or end the violation within the time specified by Contractor; or
 - b) Immediately terminate the Agreement if the Department has breached a material term of the Exhibit F, Part I and cure is not possible.
- 14) **Sanctions and/or Penalties.** Contractor understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Contractors may result in the imposition of sanctions and/or penalties on Contractor under HIPAA, the HITECH Act and the HIPAA regulations.

E. Obligations of the Department

The Department agrees to:

- 1) **Permission by Individuals for Use and Disclosure of PHI.** Provide the Contractor with any changes in, or revocation of, permission by an Individual to use or disclose Department PHI, if such changes affect the Contractor's permitted or required uses and disclosures.
- 2) **Notification of Restrictions.** Notify the Contractor of any restriction to the use or disclosure of Department PHI that the Department has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the Contractor's use or disclosure of PHI.
- 3) **Requests Conflicting with HIPAA Rules.** Not request the Contractor to use or disclose Department PHI in any manner that would not be permissible under the HIPAA regulations if done by the Department.
- 4) **Notice of Privacy Practices.** Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 C.F.R. § 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 right column and "Notice of Privacy Practices" on the right side of the page).

F. Audits, Inspection and Enforcement

If Contractor is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of

EXHIBIT F**Privacy and Information Security Provisions**

Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Exhibit F, Part I, Contractor shall notify the Department. Upon request from the Department, Contractor shall provide the Department with a copy of any Department PHI that Contractor, as the Business Associate, provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI to the Secretary. Contractor is responsible for any civil penalties assessed due to an audit or investigation of Contractor, in accordance with 42 U.S.C. § 17934(c).

G. Termination

- 1) **Term.** The Term of this Exhibit F, Part I, shall extend beyond the termination of the Agreement and shall terminate when all Department PHI is destroyed or returned to the Department, in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(I).
- 2) **Termination for Cause.** In accordance with 45 C.F.R. § 164.504(e)(1)(ii), upon the Department's knowledge of a material breach or violation of this Exhibit F, Part I, by Contractor, the Department shall:
 - a) Provide an opportunity for Contractor to cure the breach or end the violation and terminate this Agreement if Contractor does not cure the breach or end the violation within the time specified by the Department; or
 - b) Immediately terminate this Agreement if Contractor has breached a material term of this Exhibit F, Part I, and cure is not possible.

EXHIBIT F**Privacy and Information Security Provisions****Part II: Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA****1. Recitals**

- A. In addition to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the Department is subject to various other legal and contractual requirements with respect to the personal information (PI) and personally identifiable information (PII) it maintains. These include:
- 1) The California Information Practices Act of 1977 (California Civil Code §§ 1798 et seq.).
 - 2) The Agreement between the Social Security Administration (SSA) and the Department, known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency. The IEA, including the CMPPA, is attached to this Exhibit F as Attachment B and is hereby incorporated in this Agreement.
- B. The purpose of this Exhibit F, Part II is to set forth Contractor's privacy and security obligations with respect to PI and PII that Contractor may create, receive, maintain, use, or disclose for or on behalf of Department pursuant to this Agreement. Specifically this Exhibit applies to PI and PII which is not Protected Health Information (PHI) as defined by HIPAA and therefore is not addressed in Exhibit F, Part I of this Agreement, the HIPAA Business Associate Addendum.
- C. The IEA Agreement referenced in A.2) above requires the Department to extend its substantive privacy and security terms to subcontractors who receive data provided to DHCS by the Social Security Administration. If Contractor receives data from DHCS that includes data provided to DHCS by the Social Security Administration, Contractor must comply with the following specific sections of the IEA Agreement: E. Security Procedures, F. Contractor/Agent Responsibilities, and G. Safeguarding and Reporting Responsibilities for Personally Identifiable Information ("PII"), and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the Social Security Administration. Contractor must also ensure that any agents, including a subcontractor, to whom it provides DHCS data that includes data provided by the Social Security Administration, agree to the same requirements for privacy and security safeguards for such confidential data that apply to Contractor with respect to such information.
- D. The terms used in this Exhibit F, Part II, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and

EXHIBIT F
Privacy and Information Security Provisions

Agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

2. Definitions

- A. "Breach" shall have the meaning given to such term under the IEA and CMPPA. It shall include a "PII loss" as that term is defined in the CMPPA.
- B. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code § 1798.29(d).
- C. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS).
- D. "Department PI" shall mean Personal Information, as defined below, accessed in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services specified in this Agreement on behalf of the Department.
- E. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS).
- F. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29(e) whose unauthorized access may trigger notification requirements under Civil Code § 1709.29. For purposes of this provision, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.
- G. "Personally Identifiable Information" (PII) shall have the meaning given to such term in the IEA and CMPPA.
- H. "Personal Information" (PI) shall have the meaning given to such term in California Civil Code § 1798.3(a).
- I. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII 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

EXHIBIT F
Privacy and Information Security Provisions

of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

- J. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with this Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

3. Terms of Agreement

A. Permitted Uses and Disclosures of Department PI and PII by Contractor

Except as otherwise indicated in this Exhibit F, Part II, Contractor may use or disclose Department PI only to perform functions, activities or services for or on behalf of the Department pursuant to the terms of this Agreement provided that such use or disclosure would not violate the California Information Practices Act (CIPA) if done by the Department.

B. Responsibilities of Contractor

Contractor agrees:

- 1) **Nondisclosure.** Not to use or disclose Department PI or PII other than as permitted or required by this Agreement or as required by applicable state and federal law.
- 2) **Safeguards.** To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of Section 3, Security, below. Contractor will provide DHCS with its current policies upon request.
- 3) **Security.** Contractor shall 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, Business Associate Data Security Requirements; and

EXHIBIT F**Privacy and Information Security Provisions**

- b) 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.
 - c) If the data obtained by User(s) from DHCS includes PII, User(s) shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement (IEA), which are attached as Attachment B and are incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide DHCS PII agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information.
- 4) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PI or PII by Contractor or its subcontractors in violation of this Exhibit F, Part II.
 - 5) **Contractor's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit F, Part II on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of Department PI or PII to the subcontractor.
 - 6) **Availability of Information to DHCS.** To make Department PI and PII available to the Department for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of Department PI and PII. If Contractor receives Department PII, upon request by DHCS, Contractor shall provide DHCS with a list of all employees, contractors and agents who have access to Department PII, including employees, contractors and agents of its subcontractors and agents.
 - 7) **Cooperation with DHCS.** With respect to Department PI, to cooperate with and assist the Department to the extent necessary to ensure the Department's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of Department PI, correction of

EXHIBIT F

Privacy and Information Security Provisions

errors in Department PI, production of Department PI, disclosure of a security breach involving Department PI and notice of such breach to the affected individual(s).

- 8) **Breaches and Security Incidents.** During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:
- a) **Initial Notice to the Department.** (1) To notify the Department **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured Department PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving Department PII. (2) To notify the Department **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of Department PI or PII in violation of this Agreement or this Exhibit F, Part I, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor 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 Contractor.
 - b) Notice shall be provided to the Department Program Contract Manager and the Department Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic Department PI or PII, notice shall be provided by calling the Department Information Security Officer. Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link:
<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx>
 - c) Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI , Contractor shall take:
 - i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

EXHIBIT F

Privacy and Information Security Provisions

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

- d) **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI . Within 72 hours of the discovery, Contractor shall submit an updated "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 Department Program Contract Manager and the Department Information Security Officer:

- e) **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Department Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. 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 the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten(10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. 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 "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.

- f) **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PI or PII is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in CIPA, § 1798.29(a) – (d) and as may be required under the IEA. Contractor shall bear all costs of required notifications to individuals as well as any costs associated with the breach. The Department Program Contract Manager and the Department Information Security Officer and Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications

EXHIBIT F

Privacy and Information Security Provisions

are made. The Department will provide its review and approval expeditiously and without unreasonable delay. If Contractor 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 the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

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

Department Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
See the Exhibit A, Scope of Work 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	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Service Desk (916) 440-7000 or (800)

- 9. **Designation of Individual Responsible for Security.** Contractor shall designate an individual, (e.g., Security Officer), to oversee its data security program who shall be responsible for carrying out the requirements of this Exhibit F, Part II and for communicating on security matters with the Department.

EXHIBIT F
Privacy and Information Security Provisions

Part III: Miscellaneous Terms and Conditions Applicable to Exhibit F

1. Disclaimer

The Department makes no warranty or representation that compliance by Contractor with this Exhibit F, HIPAA or the HIPAA regulations will be adequate or satisfactory for Contractor's own purposes or that any information in Contractor's possession or control, or transmitted or received by Contractor, is or will be secure from unauthorized use or disclosure. Contractor is solely responsible for all decisions made by Contractor regarding the safeguarding of the Department PHI.

2. Amendment

A. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit F 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, and the HIPAA regulations. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit F embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations. The Department may terminate this Agreement upon thirty (30) days written notice in the event:

- 1) Contractor does not promptly enter into negotiations to amend this Exhibit F when requested by the Department pursuant to this section; or
- 2) Contractor does not enter into an amendment providing assurances regarding the safeguarding of Department PHI that the Department deems is necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

3. Judicial or Administrative Proceedings

Contractor will notify the Department if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. The Department may terminate this Agreement if Contractor is found guilty of a criminal violation of HIPAA. The Department may terminate this Agreement if a finding or stipulation that the Contractor 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 Contractor is a party or has been joined. DHCS will consider the nature and seriousness of the violation in deciding whether or not to terminate the Agreement.

4. Assistance in Litigation or Administrative Proceedings

Contractor shall make itself and any subcontractors, employees or agents assisting Contractor in the performance of its obligations under this Agreement, available to the

EXHIBIT F**Privacy and Information Security Provisions**

Department at no cost to the Department to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Department, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, employee or agent is a named adverse party.

5. No Third-Party Beneficiaries

Nothing express or implied in the terms and conditions of this Exhibit F is intended to confer, nor shall anything herein confer, upon any person other than the Department or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

6. Interpretation

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

7. Conflict

In case of a conflict between any applicable privacy or security rules, laws, regulations or 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, Contractor must comply within a reasonable period of time with changes to these standards that occur after the effective date of this Agreement.

8. Regulatory References

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

9. Survival

The respective rights and obligations of Contractor under Section 3, Item D of Exhibit F, Part I, Responsibilities of Contractor, shall survive the termination or expiration of this Agreement.

10. 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.

11. Audits, Inspection and Enforcement

EXHIBIT F
Privacy and Information Security Provisions

From time to time, and subject to all applicable federal and state privacy and security laws and regulations, the Department may conduct a reasonable inspection of the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit F. Contractor shall promptly remedy any violation of any provision of this Exhibit F. The fact that the Department inspects, or fails to inspect, or has the right to inspect, Contractor's facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Exhibit F. The Department's failure to detect a non-compliant practice, or a failure to report a detected non-compliant practice to Contractor does not constitute acceptance of such practice or a waiver of the Department's enforcement rights under this Agreement, including this Exhibit F.

12. Due Diligence

Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit F 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 Exhibit F.

13. Term

The Term of this Exhibit F shall extend beyond the termination of the Agreement and shall terminate when all Department PHI is destroyed or returned to the Department, in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(I), and when all Department PI and PII is destroyed in accordance with Attachment A.

14. Effect of Termination

Upon termination or expiration of this Agreement for any reason, Contractor shall return or destroy all Department PHI, PI and PII that Contractor still maintains in any form, and shall retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Contractor shall notify the Department of the conditions that make the return or destruction infeasible, and the Department and Contractor shall determine the terms and conditions under which Contractor may retain the PHI, PI or PII. Contractor shall continue to extend the protections of this Exhibit F to such Department PHI, PI and PII, and shall limit further use of such data to those purposes that make the return or destruction of such data infeasible. This provision shall apply to Department PHI, PI and PII that is in the possession of subcontractors or agents of Contractor.

EXHIBIT F
Privacy and Information Security Provisions

Attachment A**Business Associate Data Security Requirements****1. Personnel Controls**

- A. **Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of the Department, or access or disclose Department PHI or PI must complete information privacy and security training, at least annually, at Contractor'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 termination of this Agreement.
- 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 Department 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 Department PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for Department inspection for a period of six (6) years following termination of this Agreement.
- D. **Background Check.** Before a member of the workforce may access Department PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years.

2. Technical Security Controls

- A. **Workstation/Laptop encryption.** All workstations and laptops that store Department PHI or PI either directly or temporarily 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 Department Information Security Office.
- B. **Server Security.** Servers containing unencrypted Department 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.

EXHIBIT F**Privacy and Information Security Provisions**

- C. **Minimum Necessary.** Only the minimum necessary amount of Department PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. **Removable media devices.** All electronic files that contain Department PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.
- E. **Antivirus software.** All workstations, laptops and other systems that process and/or store Department 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 Department 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. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.
- G. **User IDs and Password Controls.** All users must be issued a unique user name for accessing Department 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. 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 at least 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:
- 1) Upper case letters (A-Z)
 - 2) Lower case letters (a-z)
 - 3) Arabic numerals (0-9)
 - 4) Non-alphanumeric characters (punctuation symbols)
- H. **Data Destruction.** When no longer needed, all Department PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the Department Information Security Office.

EXHIBIT F**Privacy and Information Security Provisions**

- I. **System Timeout.** The system providing access to Department 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 Department 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 Department PHI or PI, or which alters Department 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 Department 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 Department PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.
 - M. **Transmission encryption.** All data transmissions of Department 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 Department PHI can be encrypted. This requirement pertains to any type of Department 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 Department PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.
3. **Audit Controls**
- A. **System Security Review.** Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Department 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 Department 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 Department PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

EXHIBIT F
Privacy and Information Security Provisions

4. 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 Department PHI or PI held in an electronic format 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 Department PHI to maintain retrievable exact copies of Department 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 Department PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of Department data.

5. Paper Document Controls

- A. **Supervision of Data.** Department 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. Department 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 Department PHI or PI is contained shall be escorted and Department PHI or PI shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** Department PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. **Removal of Data.** Only the minimum necessary Department PHI or PI may be removed from the premises of the Contractor except with express written permission of the Department. Department PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Contractor's locations to another of Contractor's locations.
- E. **Faxing.** Faxes containing Department 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 containing Department PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible.

EXHIBIT F

Privacy and Information Security Provisions

Mailings which include 500 or more individually identifiable records of Department 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 the Department to use another method is obtained.