BOS No. Orig: #16-143; Amd1: #19-180; Amd2: #20-156
Infor PO No. 2032
Infor Ref No. 2020-2017-TPC-01

THIRD AMENDMENT
(BOS Agreement No. ____-____)

This Third Amendment to Agreement No. 16-143 ("Third Amendment") is made and entered into as of the last date signed below, by and between the County of Yolo, a political subdivision of the State of California (County), and Turning Point Community Programs, a non-profit corporation authorized to do business in the State of California (Contractor), jointly referred to as the "Parties" herein and who agree as follows.

WHEREAS, on or about September 13, 2016, the Parties entered into Agreement No. 16-143 ("Agreement"); and

WHEREAS, on or about September 10, 2019, the Parties amended the Agreement via the First Amendment; and

WHEREAS, on or about June 23, 2020, the Parties further amended the Agreement via the Second Amendment); and

WHEREAS, on or about August 26, 2020, the County exercised a portion of its option to extend the Agreement to December 31, 2020 via Option Letter #1; and

WHEREAS, on or about December 20, 2020, the County rescinded Option Letter #1 and issued a revised option notice to exercise its full option to extend the Agreement to June 30,2021 via Revised Option Letter #1; and

WHEREAS, the Parties would now like to amend the Agreement, as previously amended, to:

1. Revise **Paragraph I.A.** to update the term of the Agreement through July 31, 2021; and
2. Revise **Section II.** to update compliance requirements; and
3. Revise **Section III.** to:
   a. add funding in the amount of a $70,228.96 for FY2021-22 for a new contract maximum of $5,285,411.96; and
   b. revise the language regarding administrative costs to add references to salaries, wages, benefits and taxes; and
   c. remove references to budget shifts to align with current County policy regarding contracting authority for Department Heads; and
4. Revise **Section V.** to update exhibit and attachment(s) list; and
5. Rename **Section III.** of **Exhibit B**; and
6. Revise **Paragraph III.H.** of **Exhibit B** to update required information of the grievances and appeals log; and
7. Revise **Section IV.** of **Exhibit B** to update criteria for medical necessity, number sections for ease of reference and add an Email address to obtain copies of the Clinical Documentation Guide; and
8. Revise **Section V.** of **Exhibit B** to renumber sections for ease of reference; and
9. Revise **Paragraph VII.C.2.** of **Exhibit B**; and
10. Revise **Paragraph VII.D.** of **Exhibit B** to update progress note requirements; and

11. Revise **Paragraph VII.E. of Exhibit B** to add an Email address that may be used to obtain a copy of the Clinical Documentation Guide and update language; and

12. Revise **Exhibit C** to update language and add tracking and claim requirements for services provided during the month of June 2021 and July 2021; and

13. Rename **Section III.** of **Exhibit D** and revise to update language and the requirements of records, retention and review; and

14. Revise **Section IV.** of **Exhibit D** to update language; and

15. Revise **Paragraph V.A.** of **Exhibit D** to update language and the audit requirements; and

16. Revise **Section VI.** of **Exhibit D** to renumber sections and update language; and

17. Revise **Section IX.** of **Exhibit D** to renumber sections and update language; and

18. Revise **Section X.** of **Exhibit D** to update the dispute process and provide an email and web address for additional guidance and information on the process; and

19. Revise **Section XV.** of **Exhibit D** to update and add language; and

20. Revise **Exhibit E** to update the FY2019-20 budget with no changes in the total and add a budget for FY2021-22; and

21. Rename and revise **Exhibit F** to update language and HIPAA requirements; and

22. Add **Attachment III.**

NOW, THEREFORE, IT IS HEREBY AGREED AS FOLLOWS:

1. **Paragraph I.A.** of the Agreement is hereby amended to read as follows:

A. The term of this Agreement shall be from **July 1, 2016 through July 31, 2021** unless sooner terminated as provided in this Agreement.

2. **Section II.** of the Agreement is hereby amended to read as follows:

II. SERVICES

A. Contractor shall furnish and perform the specialty mental health services [as defined in the California Code of Regulations Title 9, Chapter 11 ("C.C.R.")] set forth in the Scope of Services attached to this Agreement as Exhibit A, in conformance with this Agreement (including, but not limited to, all exhibits), and in a manner satisfactory to the Director.

B. Contractor shall comply with all applicable provisions of State and Federal regulations and provisions as incorporated herein as if fully set forth in this place, including those founds in the State Agreements.

C. Contractor shall also comply with all applicable provisions of the HHSA Mental Health Clinical Documentation Standards Manual 2019 and the HHSA Mental Health Clinical Documentation Companion Guide 2019 (collectively hereinafter referred to as the "Clinical Documentation Guide"), the HHSA Behavioral Health Compliance Plan; and any and all applicable County policies and procedures. The Contractor has accessed and reviewed all documents, which are available to the Contractor at website http://www.yolocounty.org/health-human-services, and are incorporated herein by this reference. Contractor may also send an email to Health and Human Services Agency (HHSA)-Behavioral Health Quality Management at HHSAQualityManagement@yolocounty.org to obtain copies of any of these documents.

3. **Section III.** of the Agreement is hereby amended to read as follows:

III. COMPENSATION AND PAYMENT TERMS

A. Subject to the satisfactory performance of the services required of Contractor pursuant to this Agreement, and to the terms and conditions set forth in this Agreement, and following Contractor's submission of an appropriate claim, and such other documentation that the County may require, County shall pay Contractor according to the terms set forth in Exhibit C, Terms of Payment. Contractor agrees to accept the foregoing payments as full and complete payment for all services provided pursuant to this Agreement, irrespective of whether the cost of such services and related administrative expenses exceed such payments.

B. Any other provision of this Agreement notwithstanding, the maximum payment obligation to Contractor through **June 30, 2021** shall be no greater than **FIVE MILLION TWO HUNDERED EIGHTY-FIVE THOUSAND FOUR HUNDRED ELEVEN DOLLARS AND NINETY-SIX CENTS($5,285,411.96)** specified as follows:

Fiscal Year	MHSA Funding
Fiscal Year 2016-17 July 1, 2016 through June 30, 2017	$1,011,525
Fiscal Year 2017-18 July 1, 2017 through June 30, 2018	$1,011,525
Fiscal Year 2018-19 July 1, 2018 through June 30, 2019	$1,011,525
Fiscal Year 2019-20 July 1, 2019 through June 30, 2020	$1,090,304
Fiscal Year 2020-21 July 1, 2020 through June 30, 2021	$1,090,304
Fiscal Year 2021-22 July 1, 2021 through July 31, 2021	$70,228.96
Total	**$5,285,411.96**

C. Administrative/indirect costs shall not exceed 15% of personnel costs calculated based on salaries, wages, benefits and taxes.

D. County shall pay Contractor using a combination of funding sources, as the County deems appropriate.

4. **Section V.** of the Agreement is hereby amended to read as follows:

V. ENTIRE AGREEMENT

A. The complete Agreement shall include the following exhibits and attachment(s), attached hereto and incorporated herein by this reference:

EXHIBIT A – Scope of Services
EXHIBIT B – Medi-Cal Requirements
EXHIBIT C – Terms of Payment
EXHIBIT D – Terms and Conditions
EXHIBIT E – Contract Budget
EXHIBIT F – HIPAA Compliance, including Attachment III – *State Agreement Information Confidentiality, Security, and Privacy Requirements*
EXHIBIT G – Performance Measures

EXHIBIT H – Provider Disclosure Statement
ATTACHMENT I – RFP
ATTACHMENT II – Contractor Proposal
ATTACHMENT III – State Agreement Information Confidentiality, Security, and Privacy Requirements

The County and Contractor shall each comply with all the terms and conditions set forth in these exhibits and attachment(s). In the event of any conflict between any of the provisions of this Agreement (including Exhibits and attachments), the provision that requires the highest level of performance from Contractor for the County's benefit shall prevail.

B. This Agreement constitutes the entire agreement between the County and Contractor and supersedes all prior negotiations, representations, or agreements, whether written or oral. In the event of a dispute between the Parties as to the language of this Agreement or the construction or meaning of any term hereof, this Agreement shall be deemed to have been drafted by the Parties in equal parts so that no presumptions or inferences concerning its terms or interpretation may be construed against any party to this Agreement.

5. **Section III.** of **Exhibit B** to the Agreement is hereby renamed as follows:

III. CLIENT RIGHTS

6. **Paragraph III.H.** of **Exhibit B** to the Agreement is hereby amended to read as follows:

H. **1.** Contractor shall keep a log of all grievances and appeals, which shall contain:

- **a.** the date and time of receipt of the grievance or appeal;
- **b.** the name of the beneficiary filing the grievance or appeal;
- **c.** the name of the representative recording the grievance or appeal;
- **d.** a description of the complaint or problem;
- **e.** a description of the action taken by the plan or provider to investigate and resolve the grievance or appeal;
- **f.** the proposed resolution by the plan or provider;
- **g.** the name of the Plan provider or staff responsible for resolving the grievance or appeal;
- **h.** the date of notification to the beneficiary of the resolution.

2. Contractor shall forward the above information regarding any grievance to the County as it occurs.

7. **Section IV.** of **Exhibit B** to the Agreement is hereby amended to read as follows:

IV. MEDICAL NECESSITY CRITERIA

A. For clients to be served by Contractor, they must meet Medical Necessity Criteria as outlined in Title 9, Article 2, Section 1830.205, or Title 9, Article 2, Section 1830.210, California Code of Regulations. This information is also in the Clinical Documentation Guide.

B. Medical necessity, as defined in the above sections, must be documented clearly in each service provided to the client. If the client no longer meets medical necessity standards, services to the client must be terminated. Further, any services provided to individuals determined to not meet medical necessity will be denied.

Contractor may send an email to Health and Human Services Agency (HHSA)-Behavioral Health Quality Management at HHSAQualityManagement@yolocounty.org to obtain copies of the Clinical Documentation Guide.

8. **Section V. of Exhibit B** to the Agreement is hereby amended to read as follows:

V. ASSESSMENT

County requires an Assessment and History form that together meets the current DHCS requirements. The following areas are described by DHCS as a part of a comprehensive client record.

A. Relevant physical health conditions reported by client are prominently identified and updated as appropriate.

B. Presenting problems and relevant conditions affecting the client's physical health and mental health status are documented, for example: living situation, daily activities, and social support.

C. Documentation describes client strengths in achieving Client Plan goals.

D. Special status situations that present a risk to client or others are prominently documented and updated as appropriate.

E. Documentation includes medications that have been prescribed by MH Plan physicians, dosages of each medication, dates of initial prescriptions and refills, and documentation of informed consent for medications.

F. Client self-report of allergies and adverse reactions to medications or lack of known allergies/sensitivities are clearly documented.

G. A mental health history is documented, including but not limited to: previous treatment dates, providers, therapeutic interventions and responses, sources of clinical data, relevant family information and relevant results of relevant lab tests and consultation reports.

H. For children and adolescents, pre-natal and peri-natal events and a complete developmental history are documented.

I. Documentation includes past and present use of tobacco, alcohol, and caffeine, as well as illicit, prescribed and over-the-counter drugs.

J. A relevant mental status examination is documented.

K. A complete diagnosis from the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5), or a diagnosis from the International Classification of Diseases (ICD, Version 10), is documented consistent with the presenting problems, history, mental status evaluation and/or other assessment data.

L. Include the following:

1. Functional impairments
2. Medical necessity criteria re: evidence of Severe Emotional Disturbance or Severe Mental Illness
3. Mental status examination
4. Signature of clinician (co-signature if not licensed)

M. The requirement as to the use of the specific versions of DSM and ICD may be changed during the term of this contract. As changes occur, Contractor shall comply with the changed requirements accordingly.

9. **Paragraph VII.C.2.** of **Exhibit B** to the Agreement is hereby amended to read as follows:

   2. Each shift:
      a. Crisis Residential
      b. Crisis Stabilization
      c. Psychiatric Health Facility notes

10. **Paragraph VII.D.** of **Exhibit B** to the Agreement is hereby amended to read as follows:

   D. Other Progress Note Requirements:

   1. All entries to the beneficiary record shall be legible.
   2. All entries in the beneficiary record shall include:
      a. The date of service
      b. The signature of the person providing the service (or electronic equivalent); the person's type of professional degree, licensure or job title; and the relevant identification number, if applicable.
      c. The date the documentation was entered in the beneficiary record.
   3. The Contractor shall have a written definition of what constitutes a long-term care beneficiary.

11. **Paragraph VII.E. of Exhibit B** to the Agreement is hereby amended to read as follows:

   E. Timeliness of Progress Notes:

   1. Progress Notes shall be written or dictated within five (5) working days of the services provided and shall follow the protocol set forth in the current Clinical Documentation Guide. Contractor may send an email to HHSA-Behavioral Health Quality Management at HHSAQualityManagement@yolocounty.org to obtain a copy of the Clinical Documentation Guide.

   2. Weekly Summaries shall be due by the following Friday for Day Rehabilitation, Day Treatment Intensive, and Adult Residential.

   3. Shift Notes shall be due at the end of shift for Crisis Residential and Crisis Stabilization.

12. **Exhibit C** to the Agreement is hereby amended to read as attached.

13. **Section III.** of **Exhibit D** to the Agreement is hereby renamed and amended to read as follows:

   III. RECORDS: RETENTION AND REVIEW

   A. Records include, but are not limited to, financial and client records as described below and all other physical and electronic records and documents originated or prepared pursuant to Contractor's performance under this Agreement including but not limited to: working papers, reports, financial records and documents of account, client records, prescription files, subcontracts, and any other documentation pertaining to covered services and other related services for clients.

B. **Financial Records**

1. Contractor shall maintain financial records and other evidence, sufficient to support all direct and indirect costs of whatever nature that are claimed to have been incurred in the performance of this Agreement. These may include, but are not limited to, complete client service and financial records, which clearly reflect the actual cost and related fees received for each type of service for which payment is claimed, books, accounting procedures and practices, and audit work papers.

2. All financial records shall be retained by Contractor for whichever period of time listed below is longer:

a. at least ten (10) years from the term end date of the State Managed Care MHP Agreement, under which this Agreement is funded; or in the event the County has been notified that an audit or investigation of the State Managed Care MHP Agreement, until such time as the matter under audit or investigation has been resolved, including the exhaustion of all legal remedies, whichever is later. County will notify the Contractor if such event occurs. Contractor shall comply with the Federal and State requirements as to retaining financial records; or

b. at least ten (10) years from the date of final payment funded by Mental Health Services Act funding under this Agreement, and for such longer period, if any, as is required by applicable statute, by any other provision of the State Performance. Agreement, or if any litigation, claim, negotiation, audit, or other action involving the records has been started before the expiration of the ten-year period, the records shall be retained until completion of the action and resolution of all issues which arise from it.

C. **Client Records**

1. If applicable, Contractor shall maintain adequate client records for each client, in sufficient detail to permit an evaluation of services, which shall include, but not be limited to, the following: admission information, demographic information, consent for treatment, medical history, assessment and diagnostic studies, client plan, records of patient interviews, and records of all services provided. Additional requirements for an assessment, client plan, and progress notes are specified in the Quality Management Standards set forth in Exhibit B. Such records shall also comply with all applicable Federal, State, and County record retention requirements. If applicable, Contractor shall comply with the Federal, State and County requirements as to maintaining electronic health records. County and Contractor will collaborate to provide patients with access to patient healthcare records in compliance with all applicable Federal, State, and County regulations.

2. All client records shall be kept for whichever time period listed below is longer:

a. at least ten (10) years from the term end date of the State Managed Care MHP Agreement, under which this Agreement is funded; or in the event the County has been notified that an audit or investigation of the State Managed Care MHP Agreement, until such time as the matter under audit or investigation has been resolved, including the exhaustion of all legal remedies, whichever is later. County will notify the Contractor if such event occurs. Contractor shall comply with the Federal and State requirements as to retaining financial records; or

b. at least ten (10) years from the date of final payment funded by Mental Health Services Act funding under this Agreement, and for such longer period, if any, as is required by applicable statute, by any other provision of the State Performance.

Agreement, or if any litigation, claim, negotiation, audit, or other action involving the records has been started before the expiration of the ten-year period, the records shall be retained until completion of the action and resolution of all issues which arise from it.

c. a minimum of ten (10) years from the patient's date of discharge, if the patient is eighteen (18) years old or older when they are discharged; or

d. until the patient's 28th birthday, if the patient was treated and discharged while they were a minor; or

e. if the patient was pregnant at the time of treatment, patient's records shall be maintained for 25 years from last date of treatment while pregnant. In the event the client was pregnant more than once while they received treatment, the last date of treatment of the last pregnancy shall be used to calculate the appropriate time frames for record retention. If the last day of treatment while pregnant cannot be ascertained from the client record, the last day of treatment while pregnant shall be calculated as one year from the initial report of pregnancy in the client record.

D. If Contractor ceases to provide the services required by this Agreement for any reason, Contractor will contact County and make appropriate arrangements for transfer of care of the clients and for County to take possession of client records. Electronic health care records shall be made available to the County in an electronic format readable by the County.

E. Contractor may, at its discretion, following receipt of final payment under this Agreement, reduce its accounts, books, and records related to this Agreement to microfilm, computer disk, CD ROM, DVD, or other data storage medium. Upon request by an authorized representative to inspect, audit or obtain copies of said records, Contractor must supply or make available applicable devices, hardware, and/or software necessary to view, copy, and/or print said records. Applicable devices may include, but are not limited to, microfilm readers and microfilm printers, etc.

F. This section shall survive the termination or completion of this Agreement for the full period of time allowed by law.

14. Section IV. of **Exhibit D** to the Agreement is hereby amended to read as follows:

IV. REPORTS

A. Contractor shall submit to County the following listed reports. Contractor shall make further reports as may be reasonably requested by Director, the State and/or Federal government concerning Contractor's activities as they affect the services and obligations required by this Agreement. All reports must be submitted as prescribed by this Agreement or as otherwise reasonably requested by the Director.

B. Practitioner Information Report:

1. NPI/License List
Practitioners must obtain a NPI prior to first day of service. A copy of current license and NPI provider registry date printout must be submitted to Yolo County Health and Human Services Agency. Note that the practitioner's legal name must appear on both the current license and NPI printout. The NPI printout may be accessed at: https://npiregistry.cms.hhs.gov/.

2. Practitioner ID Enrollment Form
A complete Practitioner Enrollment Form, which is available on the Yolo County website, must be provided for all personnel for the first month of this Agreement, and thereafter, for new personnel immediately upon hire or changed information.

Each Practitioner Enrollment form must be accompanied with required supporting documents and a copy of current license and NPI provider registry date printout. Note that the practitioner's legal name must appear on both the current license and NPI printout. The NPI printout may be accessed at: https://npiregistry.cms.hhs.gov/.

For staff to be classified as Mental Health Rehabilitation Specialist (MHRS), the Practitioner Enrollment Request form must also be accompanied with a completed MHW-MHRS classification application and the staff must meet the minimum regulatory requirements set forth in the California Code of Regulations, 9 CCR § 630, which states:

> **§ 630. Mental Health Rehabilitation Specialist.**
> A mental health rehabilitation specialist shall be an individual who has a baccalaureate degree and four years of experience in a mental health setting as a specialist in the fields of physical restoration, social adjustment, or vocational adjustment. Up to two years of graduate professional education may be substituted for the experience requirement on a year-for-year basis; up to two years of post-associate arts clinical experience may be substituted for the required educational experience in addition to the requirement of four years' experience in a mental health setting. (9 CCR § 630).

The Practitioner Enrollment form and accompanying documentation must be submitted to Yolo County Health and Human Services Agency for approval prior to first day of service. Submit these reports electronically via email to: HHSAQualityManagement@yolocounty.org

C. Employee Verification Report: (See Section II. of this Exhibit.)
Contractor shall verify prior to hire that all of Contractor's employees and subcontractors are eligible to provide services under this Agreement pursuant to all applicable state and federal rules, including applicable sections of the State Contracts. Contractor shall maintain documentation of verification on file and provide such documentation to County upon request.

D. Performance Outcome Measures (POM) Report: (See Exhibit G of this Agreement.)
Contractor shall maintain data and reports of performance outcome measures in compliance with the Federal and State requirements. On a bi-annual basis, Contractor shall make these data and reports available to the County, as specified in Exhibit G, Performance Measures.

Submit the Performance Outcome Measures electronically via email to: HHSAQualityManagement@yolocounty.org

E. Contract Expenditure Reports
The Contract Expenditure Reports include the Mid-Year Report and the End of Year Report as described, below:

1. *Mid-Year Report*: This includes the total contract expenditures for the period of July 1 through December 31 and year-to-date information on actual expenditures and revenues. To be submitted by January 31st.

2. *End of Year Report*: This includes contract expenditures for the period of July 1 through June 30 and year end information on actual expenditures and revenues. To be submitted by July 31st.

Submit the Contract Expenditures Reports electronically via email to: HHSA.AccountsPayable@yolocounty.org .

F. Fiscal Year Annual Reports

1. *Annual Training Report:* This report summarizes all training provided to Contractor's staff and all outreach training performed by Contractor's staff. Due date: July 31, following the completion of a fiscal year

2. *Aggregated Staff and Volunteer Ethnicity Survey:* An Individual Staff and Volunteer Ethnicity Survey form will be provided as a tool to accumulate data to be compiled into the aggregated report.
Due date: November 30, following the completion of a fiscal year

3. *Equipment Report* (See Section VII. Ownership of Equipment, below.) Due date: July 31, following the completion of a fiscal year

4. *Certified Mental Health Cost Report* (see Section XXX. Cost Settlement, below.) Due date: October 31, following the completion of a fiscal year (June 30) unless the Agreement is terminated or expires earlier. If the Agreement expires or is terminated before June 30, then the Cost Report is due, no later than forty-five (45) days from the date of the expiration or termination.

5. *Certified Audited Financial Reports* (see Section V. Audit) Due date: June 30, following the completion of next fiscal year, i.e., two hundred seventy (270) days following the above said due date for the Certified Mental Health Cost Report unless the Agreement is terminated or expires earlier. If the Agreement expires or is terminated before June 30, then the Certified Audited Financial Reports are due, no later than forty-five (45) days from the date of the expiration or termination.

All annual reports, with the exception of Certified Mental Health Cost Report and Certified Audited Financial Reports, shall be sent electronically via email to the Contract Administrator. (See Section XVIII. NOTICES.)

The Certified Mental Health Cost Report and Certified Audited Financial Reports shall be sent to:

Yolo County Health and Human Services Agency
137 N. Cottonwood Street
Woodland, CA 95695
Attn: Cost Report

15. Paragraph V.A. of **Exhibit D** to the Agreement is hereby amended to read as follows:

A. Contractor shall allow the County, California Department of Healthcare Services, Centers and the Bureau of State Audits, and any other authorized federal and state agencies, or their duly authorized designees, to evaluate Contractor's performance under this contract, including the quality, appropriateness, and timeliness of services provided, and to inspect, evaluate, and audit any and all records, documents, and the premises, equipment and facilities maintained by the Contractor and its subcontractors pertaining to such services at any time.

Contractor shall allow such inspection, evaluation and audit of its records, documents and facilities, and those of its subcontractors, for 10 years from the term end date of this Contract or in the event the

Contractor has been notified that an audit or investigation of this Contract has been commenced, until such time as the matter under audit or investigation has been resolved, including the exhaustion of all legal remedies, whichever is later. (For the State Managed Care MHP Agreement services, see 42 C.F.R. §§ 438.3(h), 438.230(c)(3)(i-iii).) Records are defined in Section III.A., above.

Any failure or refusal by Contractor to permit access to records by the County, California Department of HealthCare Services, and the Bureau of State Audits, and any other authorized federal and state agencies, or their duly authorized designees, as otherwise provided by this Agreement, the State Contracts, State and/or Federal laws and regulations, shall constitute an express and immediate breach of this Agreement.

The Contractor shall also be subject to the examination and audit of the Auditor General for a period of three (3) years after final payment under contract (Government Code, Section 8546.7).

16. **Section VI.** of **Exhibit D** to the Agreement is hereby amended to read as follows:

VI. CULTURAL COMPETENCY

A. Cultural competence is defined as a set of congruent practice behaviors, attitudes, and policies that come together in a system, agency, or among consumer providers and professionals which enable that system, agency, or those professional and consumer providers to work effectively in cross-cultural situations.

B. Contractor recognizes that cultural competence is a goal toward which professionals, agencies, and systems should strive. Becoming culturally competent is a developmental process and incorporates at all levels the importance of culture, the assessment of cross-cultural differences, the expansion of cultural knowledge, and the adaptation of services to meet culturally unique needs. Providing medically necessary specialty behavioral health, substance abuse, and co-occurring disorder services in a culturally competent manner is fundamental in any effort to ensure success of high quality and cost-effective services. Offering those services in a manner that fails to achieve its intended result due to cultural and linguistic barriers is not cost effective.

C. Contractor shall assess the demographic make-up and population trends of its service area to identify the cultural and linguistic needs of the eligible beneficiary population. Such studies are critical to designing and planning for providing appropriate and effective behavioral health, substance abuse, and co-occurring disorder services.

D. Contractor shall implement practices and protocols that are inclusive and responsive to the needs of diverse cultural populations, including Lesbian, Gay, Bisexual, Transgender and Queer/Questioning (LGBTQ) individuals, families and communities.

E. Contractor shall adopt the National Standards for Culturally and Linguistically Appropriate Services (CLAS) in Health and Health Care to improve health care quality and advance health equity. Refer to http://minorityhealth.hhs.gov (US Department of Health and Human Services Office of Minority Health).

F. Language Access and Translation Requirements

1. "Threshold Language" pursuant to the Dymally-Alatorre Bilingual Services Act and "Prevalent Language" pursuant to State contracts and 42 CFR. §438.10(a), means a language that has been identified as the primary language, as indicated on the Medi-Cal Eligibility System (MEDS), of 3,000 beneficiaries or five percent of the beneficiary population, whichever is lower, in County's Medi-Cal service area. (Cal.

Govt. Code §7290-7299.8; 42 CFR. §438.10(a); 9 CCR §1810.410(a)(3).)

2. Contractor shall comply with the linguistic requirements included herein.

a. The Contractor shall provide all written materials for potential clients and clients in a font size no smaller than 12 point. (42 CFR. 438.10(d)(6)(ii).)

b. The Contractor shall ensure its written materials are available in alternative formats, including large print, upon request of the potential client or client at no cost. Large print means printed in a font size no smaller than 18 point. (42 C.F.R. § 438.10(d)(3).)

c. The Contractor shall make its written materials that are critical to obtaining services, including, at a minimum, provider directories, beneficiary handbooks, appeal and grievance notices, denial and termination notices, and Contractor's behavioral health education materials, available in the prevalent non-English languages in the county. (42 CFR. § 438.10(d)(3).)

d. The Contractor shall notify clients that written translation is available in prevalent languages free of cost and shall notify clients how to access those materials. (See 42 CFR § 438.10(d)(5)(i) & (iii); 9 CCR § 1810.410(e)(4).)

i. The Contractor shall include taglines in the prevalent non-English languages in the State of California, as well as large print, explaining the availability of written translation or oral interpretation to understand the information provided. (42 CFR. § 438.10(d)(2).)

ii. The Contractor shall include taglines in the prevalent non-English languages in the State of California, as well as large print, explaining the availability of the toll-free and Teletypewriter Telephone/Text Telephone (TTY/TDY) telephone number of the Contractor's member/customer service unit. (42 CFR § 438.10(d)(3).)

iii. The Contractor shall notify clients that written translation is available in prevalent languages free of cost and shall notify clients how to access those materials. (42 C.F.R. § 438.10(d)(5)(i), (iii); Cal. Code Regs., tit. 9, § 1810.410, subd. (e), para. (4).)

e. The Contractor shall make oral interpretation and auxiliary aids and services, such as TTY/TDY and American Sign Language (ASL), available and free of charge for any language. Contractor shall notify clients that the service is available and how to access those services. (42 CFR. § 438.10(d).

17. **Section IX.** of **Exhibit D** to the Agreement is hereby amended to read as follows:

IX. CONFIDENTIALITY

Contractor shall comply with, and require its officers, agents, employees, participants, and volunteers to comply with:

A. all applicable laws and regulations regarding the confidentiality of patient information, including but not limited to California Welfare and Institutions Code Sections 5328 et seq., 10850, and 14100 et seq., 42 U.S.C. §1320d, and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the HIPAA Omnibus Rule, 45 CFR Parts 160 and 164,

and its implementing regulations, and the Federal Confidentiality of Substance Abuse Disorder Patient Records laws and regulations, Title 42 of the United States Code §290dd-2 and 42 CFR Part 2 ("Part 2 Regulations");

B. the privacy and security requirements of Exhibit F attached hereto; and

C. any additional regulations pertaining to confidentiality that the Federal, State or the County shall so specify that do not conflict with State or Federal regulations.

18. Section X. of **Exhibit D** to the Agreement is hereby amended to read as follows:

X. DISPUTES

A. For any client dispute or grievance arising from the provision of behavioral health services, Contractor shall direct client to use the County Client Problem Resolution process. Contractor find informing materials at: https://www.yolocounty.org/health-human-services/mental-health/behavioral-health-quality-management#CommunityPartner and may contact the Yolo County Health and Human Services Agency (HHSA)-Behavioral Health Quality Management Unit at HHSAQualityManagement@yolocounty.org for additional guidance on this process.

B. Any other dispute arising between the Contractor and the County relating to performance under this contract other than disputes governed by a dispute resolution process in Chapter 11 of Division 1, Title 9, California Code of Regulations (CCR), the Contractor shall, prior to exercising any other remedy which may be available, provide the County with written notice of the particulars of the dispute within thirty (30) calendar days of the incident. Upon receipt of the written notice, the County shall meet with the Contractor, review the facts in the dispute, and recommend a means of resolving the dispute. Final written response to the Contractor will be provided within thirty (30) days of receipt of the Contractor's original written notice.

19. Section XV. of **Exhibit D** to the Agreement is hereby amended to read as follows:

XV. INDEMNIFICATION

A. With the exception that this Section shall in no event be construed to require indemnification by Contractor to a greater extent than permitted under the laws or public policy of the State of California, Contractor shall indemnify, defend and hold harmless the County of Yolo and its officers, agents, employees and volunteers from and against any and all claims, damages, demands, losses, defense costs, expenses (including attorneys' fees) and liability of any kind or nature arising out of or resulting from performance of the work, provided that any such claim, damage, demand, loss, cost, expense or liability is caused in whole or in part by any negligent or intentional act or omission of the contractor, any subcontractor, anyone directly or indirectly employed by any of them or anyone for whose acts any of them may be liable, regardless of whether or not it is caused in part by a party indemnified hereunder.

B. Contractor and/or any subcontractor's responsibility for such defense and indemnity obligations shall survive the termination or completion of this Agreement for the full period of time allowed by law.

C. The defense and indemnification obligations of this Agreement are undertaken in addition to, and shall not in any way be limited by, the insurance obligations contained in this Agreement. In providing any defense under this Section, Contractor shall utilize counsel approved by the Office of the County Counsel in its reasonable discretion.

D. Any subcontractor must agree to be bound to the County of Yolo in the same manner and to the same extent as Contractor is bound to the County of Yolo under this Agreement. Any subcontractors must further agree to include the same requirements and provisions of this Agreement, including the indemnity and insurance requirements, with any sub-subcontractor to the extent they apply to the scope of the sub-subcontractor's work.

20. Exhibit E to the Agreement is hereby amended to read as attached.

21. Exhibit F to the Agreement is hereby renamed and amended to read as attached.

22. Attachment III is hereby added to the Agreement to read as attached.

23. All attachments to this Third Amendment are incorporated into this Amendment by reference above.

24. Except as specifically amended by this Third Amendment and any prior amendments, the Agreement shall remain in full force and effect according to its terms.

IN WITNESS WHEREOF, the Parties have executed this Third Amendment as of the last day and year set forth below.

CONTRACTOR

By: _____
Alfred Rowlett, Chief Executive Officer
Turning Point Community Programs

Date: 12·03·2021

COUNTY OF YOLO

By: _____
~~Jim Provenza, Chair~~ Angel Barajas, Chair
Board of Supervisors

Date: _____

Karen Larsen, Director
Health and Human Services Agency

Attest:
Julie Dachtler, Senior Deputy Clerk
Board of Supervisors

By: _____
Deputy (Seal)

Approved as to Form:
Philip J. Pogledich, County Counsel

By: Hope P. Welton
Hope P. Welton, Senior Deputy

EXHIBIT C – TERMS OF PAYMENT

I. BUDGET

A. Contractor submitted a contract budget attached hereto as Exhibit E. Contractor shall adhere to this budget in performing services that have been authorized and provided in accordance with the provisions of this Agreement.

B. Amendments to the budget including but not limited to shifting the allocation of funds between categories of services, must be mutually agreed upon in writing. Contractor shall provide a revised budget to the Director for approval. Budget amendments must be approved pursuant to Section IV. Option Year and Amendment Authority, of this Agreement.

C. In the event the County requests an updated budget for any option year, the option year budget shall be approved in conformance with Section III.B.2. of this Agreement, in the sole discretion of the HHSA Director.

II. METHOD OF PAYMENT

A. If applicable, Contractor shall determine if a client has any funding sources other than County funds, including private insurance or sufficient income to fund services. Contractor shall only bill County for client services after all other funding sources for a client have been exhausted or if a Medi-Cal or EPSDT only provider, bill accordingly. Contractor shall use due diligence in determining and collecting client and third-party payments.

B. Contractor shall submit a monthly claim in accordance with these Terms of Payment using the claim form as specified by the Director. The monthly claim will summarize the services provided during the previous month in grouping by service location, practitioner, and service code. Contractor shall provide all required supporting documentation. Supporting documentation may include, but is not necessarily limited to, written authorization for services, daily transactions certified by the individual service providers, progress notes, actual units of time and units of service, Medi-Cal swipes, approved Treatment Authorization Requests (TAR), explanation of benefits by other health care carrier, time sheets, labor distribution, general-ledger printouts, costs per line item, and they must be maintained for audit purposes.

C. 1. Yolo County HHSA shall not require prior authorization for the following services/service activities:

- **a.** Crisis Intervention;
- **b.** Crisis Stabilization;
- **c.** Mental Health Services;
- **d.** Targeted Case Management;
- **e.** Intensive Care Coordination; and,
- **f.** Medication Support Services.

However, HHSA may impose appropriate utilization controls by requiring all Assessments to be conducted by the MHP's clinical staff. In these cases, HHSA is permitted to then make a referral to a network provider for treatment. However, if the MHP delegates, to the MHP's network providers, responsibility for conducting Assessments, prior authorization is not permissible. Mental Health Services – Rehabilitation, Targeted Case Management, and Intensive Care Coordination must be included on the beneficiary's Client Plan prior to service delivery. Although Yolo County HHSA may not require prior authorization for these services, it retains the option to review and approve beneficiaries' Client Plans prior to service delivery.

3. Prior authorization or Yolo County HHSA referral is required for the following services:
   a. Intensive Home-Based Services
   b. Day Treatment Intensive
   c. Day Rehabilitation
   d. Therapeutic Behavioral Services
   e. Therapeutic Foster Care
4. For purposes of prior authorization, referral by Yolo County HHSA is considered to serve the same function as approving a request for authorization submitted by a provider or beneficiary.
5. For continuation of services, network providers shall request payment authorization for the continuation of services at the following intervals:
   1. Every three (3) months
      a. Day Treatment Intensive
      b. Therapeutic Behavioral Services
      c. Therapeutic Foster Care
   2. Every six (6) months
      a. Intensive Home Base Services
      b. Day Rehabilitation

   (See DHCS MHSUDS Information Notice: 19-026).

D. Contractor shall submit such claims for payment to the County no later than thirty (30) days after completion of the month in which services have been rendered. Claims that must first be billed to a third party, e.g. Medicare, insurance, etc., must be submitted no later than sixty (60) days after completion of the month in which services have been rendered. Any claim that is submitted and rejected due to lack of necessary information must be resubmitted within twenty (20) days of the date of the initial rejection.

E. Claims for payment may be submitted to the county in an electronic format at HHSA.AccountsPayable@yolocounty.org. All claims shall be submitted with any required supporting documentation accompanying the claim. If a claim contains confidential client information, the claim and supporting documentation must be encrypted for transmission.

Claims, with any required supporting documentation, may also be submitted via US Postal Service mail addressed to:

Yolo County Health and Human Services Agency
137 N. Cottonwood Street, Suite 2400
Woodland, CA 95695
Attn: Accounts Payable

F. **1.** For mental health and outreach and engagement services, County shall pay Contractor the amount payable calculated based on the interim rates specified below for services that have been authorized and provided in accordance with the provisions of this Agreement.

2. For other non Medi-Cal client support services provided during June 2021 and July 2021, Contractor shall track these expenses separately and identify these expenses separately on the monthly claims for payment submitted to the County. County shall pay

EXHIBIT C – TERMS OF PAYMENT

Contractor for actual expenditures incurred as supported by the documentation accompanying the claim.

Service Code	Descriptions	Rate/Unit
4510	Prop 63 Outreach and Engagement *(This is only applicable for the AOT participants.)*	$2.13/minute
90791	Assessment	$2.75/minute
H0032	Plan Development	$2.75/minute
90832	Psychotherapy (30 Min)	$2.75/minute
90834	Psychotherapy (45 Min)	$2.75/minute
90837	Psychotherapy (60 Min)	$2.75/minute
90853	Group Therapy	$2.75/minute
T1017	Targeted Case Management	$2.13/minute
97535	Rehabilitation/ADL	$2.75/minute
97535G	Group Rehabilitation	$2.75/minute
90887	Collateral	$2.75/minute
90839	Crisis Intervention	$2.75/minute
99201	E&M New Patient Office Visit: Level 1 Minimal Complexity	$4.29/minute
99202	E&M New Patient Office Visit: Level 2 Minor Problem	$4.29/minute
99203	E&M New Patient Office Visit: Level 3 Low Severity	$4.29/minute
99204	E&M New Patient Office Visit: Level 4 Moderate Severity	$4.29/minute
99205	E&M New Patient Office Visit: Level 5 High Severity	$4.29/minute
99211	E&M Established Patient Office Visit: Level 1 Minimal Complexity	$4.29/minute
99212	E&M Established Patient Office Visit: Level 2 Minor Problem	$4.29/minute
99213	E&M Established Patient Office Visit: Level 3 Low Severity	$4.29/minute
99214	E&M Established Patient Office Visit: Level 4 Moderate Severity	$4.29/minute
99215	E&M Established Patient Office Visit, Level 5 High Severity	$4.29/minute
90899	Medication Support-RN/LVN/LPT	$4.29/minute
6078	Other Non Medi-Cal Client Support	Actual Cost Reimbursement

2. The use of the codes specified above is subject to change in accordance with changes in Federal, State or County guidelines.

3. For cost reporting purpose, Contactor shall establish an internal tracking system that will accurately maintain units of service. The cost report must include all units of service-related mental health services for the County, whether paid or not by the County. Contractor shall report units of service in accordance with the State issued cost report instructions as well as any applicable regulations that govern the cost reporting.

a. Contractor shall meet the following Medi-Cal Billing Targets.

Medi-Cal Billing Targets

Target Annual Billable Services	$1,665,304.00
Target Annual Billable Units	$ 380,237.00
Target Monthly Billable Services	$ 138,775.34
Target Monthly Billable Units	$ 31,686.42
Target Annual Non-Billable Services	$0
Target Annual Non-Billable Units	$ 20,580.00
Target Monthly Non-Billable Services	$0
Target Monthly Non-Billable Units	$ 1,715.00
Total Contract Amount	$1,665,304.00

4. To meet the MHSA reporting requirements, Contractor shall submit claims and differentiate the costs as to the MHSA categories, e.g., Full-Service Partnership, General System Development, and Outreach as well as the specific MHSA programs, e.g. Transitional Youth, Adult, Older Adult, etc.

G. Final compensation to the Contractor shall be at the actual rate and the total compensation shall not exceed the maximum payable set forth in Section III of this Agreement. County shall determine the final compensation to the Contractor based on the final audited Cost Report as specified in Sections IV and XXX of Exhibit D, at the actual rate and the total compensation shall not exceed the maximum payable set forth in Section III of this Agreement.

H. If Medi-Cal applies; County shall make payments to Contractor for services claimed by Contractor prior to billing for Federal Financial Participation (FFP) reimbursement. In the event any claim is denied/rejected by the Federal and/or State government, Contractor shall take all actions necessary to obtain such approval. If any denied claim by Federal and/or State government is not finally approved for payment reimbursement, Contractor's next payment from County shall be reduced by the amount of denied/rejected claims by Medi-Cal and Medicare. Contractor disallowances are the Contractor's fiscal and program responsibility, per Section M., below.

I. County shall authorize payment within forty-five (45) days of the receipt of Contractor's appropriate claim, required reports, and any further documentation requested by the County for purposes of this Agreement.

J. If the Contractor fails to comply with any provision of this Agreement, County may withhold payment otherwise due Contractor pursuant to this Agreement or any other agreement between Contractor and County until such noncompliance has been corrected.

K. Claims submitted one hundred eighty (180) days after the date of service will be denied in accordance with State of California regulations concerning timely submission. Late claims submitted with a written request within a reasonable timeframe before the one hundred eighty (180) day regulation cut off, if it is due to circumstances beyond the control of the Contractor, may be approved by the Director for claim submission.

L. If applicable, County shall make a diligent effort to process and submit billings to the Federal and/or State government in a timely manner. Should the Federal and/or State government deny payment to the County due to late billing, County will demand repayment from Contractor, for any such paid claim that is not submitted within the timelines as specified in the above paragraph C, irrespective if such services were claimed in the original or resubmitted claim, or such claims were withheld by County due to Contractor's noncompliance with any provision of this Agreement.

M. **1.** County will demand repayment from Contractor for compensation made to the Contractor, in the event that any goods and/or services related to such compensation are subsequently determined disallowable, regardless of reason.

2. Any such disallowance related to the current term of this Agreement will be due and payable immediately to the County. County will recoup from Contractor by offsetting any payment otherwise due Contractor pursuant to this Agreement or any other agreement between Contractor and County.

3. Any such disallowance related to the prior terms of this Agreement or any other agreement between Contractor and County will be due and payable within forty-five (45) days of mailing a demand letter from County to Contractor. Thereafter, unless otherwise negotiated with and approved by the Director, County will recoup from Contractor the amount due, by offsetting any payment otherwise due Contractor pursuant to this Agreement or any other agreement between Contractor and County.

4. In the event that the aggregated payment otherwise due Contractor pursuant to this Agreement or any other agreement between Contractor and County is less than the amount due, and when all payments otherwise due Contractor have been exhausted, Contractor shall make payment to the County for any balance due based on a payment plan negotiated with and approved by the Director.

N. Any other provision of this Agreement notwithstanding, because this Agreement is funded by the State Contracts, the County's obligation to compensate Contractor pursuant to this Agreement is contingent upon, and subject to, the County's receipt of such funding from the State, and the absence or removal of any constraints imposed by the State upon such receipt and payment.

O. Contractor shall use the funds provided by County exclusively for the purposes of performing the services required by this Agreement. No funds provided by County pursuant to this Agreement shall be used for any political activity or political contribution.

P. Contractor shall hold harmless the State and clients in the event that the County does not pay for services in accordance with this Agreement.

Q. When eligible and appropriate, the County may claim some or all services to Medi-Cal Administrative Activities (MAA) funding. When the County intends to bill for MAA reimbursement, County will provide Contractor with a required Time Study or other time or cost tracking template. In the event that County bills MAA, Contractor shall complete and return the required forms to County in the manner established by the County and within the claiming timelines.

EXHIBIT E – CONTRACT BUDGET

Turning Point Community Program		
MHSA Full-Service Partnership Services		
	Cost Items	Each County Fiscal Year for Fiscal Years 2016-17, 2017-18, 2018-19 **July 1 through June 30**
1	**a. Personnel**	**$752,522**
	b. Indirect (15%) Admin.	$99,245
2	Operating Costs	**$145,733**
3	Direct to Clients	$14,025
4	**Total**	**$1,011,525**

Turning Point Community Program		
MHSA Full-Service Partnership Services		
	Cost Items	County Fiscal Year 2019-20 **July 1 through June 30**
1	**a. Personnel**	**$831,301**
	b. Indirect (15%) Admin.	$99,245
2	Operating Costs	**$145,733**
3	Direct to Clients	$14,025
4	**Total**	**$1,090,304**

Turning Point Community Program		
MHSA Full-Service Partnership Services		
	Cost Items	County Fiscal Year 2020-21 **July 1 through June 30**
1	**a. Personnel**	**$831,301**
	b. Indirect (15%) Admin.	$99,245
2	Operating Costs	**$145,733**
3	Direct to Clients	$14,025
4	**Total**	$1,090,304

EXHIBIT E – CONTRACT BUDGET

Turning Point Community Program		
MHSA Full-Service Partnership Services		
	Cost Items	County Fiscal Year 2021-22 **July 1 through July 31**
1	a. Personnel	$0
	b. Indirect (15%) Admin.	$0
2	Operating Costs	$70,228.96
3	Direct to Clients	$0
4	Total	$70,228.96

EXHIBIT F – HIPAA COMPLIANCE

I. The County and Contractor shall protect the privacy and provide for the security of protected health information (PHI) pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the HIPAA Omnibus Rule, Title 45, Code of Federal Regulations ("C.F.R.") Parts 160 and 164, the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated there under by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws (collectively "the Privacy Laws".) The requirements of the Privacy Laws include but are not limited to: the use of methods of encryption for any electronic submissions containing PHI; and specific notice requirements should there be a security incident as defined in 45 CFR §164.304 or breach of unsecured PHI as defined by 45 CFR §164.402.

II. Pursuant to HIPAA and the other Privacy Laws, as set forth in, but not limited to, 45 CFR §§164.314(a), 164.502(e) and 164.504(e), the County and Contractor, and other third party entity or entities may be required to enter into a Business Associate Agreement or Business Associate Agreement & Qualified Service Organization Agreement containing the specific requirements regarding Contractor's acquisition, access, use, or disclosure of PHI prior to such acquisition, access, use, or disclosure of PHI. If the County determines, in its sole discretion, that a Business Associate Agreement or Business Associate Agreement & Qualified Service Organization Agreement is required, the parties mutually agree to execute same.

III. By signing this Agreement, Contractor certifies it has reviewed, understands the contents of, and shall comply with:

A. the requirements set forth in *Exhibit D – Information Confidentiality and Security Requirements* and *Exhibit E – Privacy and Information Security Provisions* of the State Performance Agreement, which are attached hereto as Attachment III and are hereby incorporated by reference.

B. the Yolo County HHSA Behavioral Health Compliance Plan, available to the Contractor at website https://www.yolocounty.org/health-human-services/mental-health/behavioral-health-quality-management/-folder-3841#docan1597_10556_7495

IV. Report, as soon as reasonably practicable, and in no event less than 24 hours for security incidents, as defined in 45 CFR §164.304, and 1 hour for breaches of unsecured PHI as defined by Section 164.402 of the HIPAA Regulations, to the County's Privacy Officer, the County's Security Officer, and to the HHSA Behavioral Health Compliance Officer HHSA.BHCompliance@yolocounty.org.

V. The provisions of this **Exhibit F** shall survive the termination, expiration, or cancellation of this Agreement.

ATTACHMENT III
Information Confidentiality and Security Requirements
(Exhibit D of the State Performance Agreement)

1. **Definitions**. For purposes of this Exhibit, the following definitions shall apply:

   A. **Public Information:** Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

   B. **Confidential Information:** Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

   C. **Sensitive Information:** Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.

   D. **Personal Information:** Information that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. **It is DHCS' policy to consider all information about individuals private unless such information is determined to be a public record.** This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. Personal Information includes the following:

      Notice-triggering Personal Information: Specific items of personal information (name plus Social Security number, driver license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. See Civil Code sections 1798.29 and 1798.82.

2. **Nondisclosure.** The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Personal Information, Sensitive Information, or Confidential Information (hereinafter identified as PSCI).

3. The Contractor and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the Contractor's obligations under this Agreement.

4. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the DHCS Program Contract Manager all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.

5. The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the person who is the subject of PSCI, any PSCI to anyone other than DHCS without prior written authorization from the DHCS Program Contract Manager, except if disclosure is required by State or Federal law.

6. The Contractor shall observe the following requirements:

   A. **Safeguards.** The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PSCI,

including electronic PSCI that it creates, receives, maintains, uses, or transmits on behalf of DHCS. 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, Including at a minimum the following safeguards:

1) Personnel Controls

a. ***Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of DHCS, or access or disclose DHCS PSCI, must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.

b. ***Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

c. ***Confidentiality Statement.*** All persons that will be working with DHCS PSCI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PSCI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.

d. ***Background Check.*** Before a member of the workforce may access DHCS PSCI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

2) Technical Security Controls

a. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store DHCS PSCI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.

b. ***Server Security.*** Servers containing unencrypted DHCS PSCI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

c. ***Minimum Necessary.*** Only the minimum necessary amount of DHCS PSCI required to perform necessary business functions may be copied, downloaded, or exported.

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

e. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store

DHCS PSCI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

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

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

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

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

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

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

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

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

m. ***Transmission encryption.*** All data transmissions of DHCS PSCI 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 PSCI can be encrypted. This requirement pertains to any type of PSCI in motion such as website access, file transfer, and E-Mail.

n. ***Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting DHCS PSCI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3) **Audit Controls**

a. ***System Security Review.*** All systems processing and/or storing DHCS PSCI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

b. ***Log Reviews.*** All systems processing and/or storing DHCS PSCI must have a routine procedure in place to review system logs for unauthorized access.

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

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 electronic DHCS PSCI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

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

5) **Paper Document Controls**

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

b. ***Escorting Visitors.*** Visitors to areas where DHCS PSCI is contained shall be escorted and DHCS PSCI shall be kept out of sight while visitors are in the area.

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

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

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

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

B. ***Security Officer.*** The Contractor shall designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with DHCS.

Discovery and Notification of Breach. Notice to DHCS:

1) To notify DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to DHCS by the Social Security Administration. This notification will be **by telephone call plus email or fax** upon the discovery of the breach. (2) To notify DHCS **within 24 hours by email or fax** of the discovery of unsecured PSCI in electronic media or in any other media if the PSCI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PSCI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by the 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 the contractor.

Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to DHCS by the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. The contractor shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

C. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PSCI, the Contractor shall take:

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

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

D. ***Investigation of Breach.*** The Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PSCI. If the initial report did not include all of the requested information marked with an asterisk, then within seventy-two (72) hours of the discovery, The Contractor shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer:

E. ***Written Report.*** The Contractor shall provide a written report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security

Officer, if all of the required information was not included in the DHCS Privacy Incident Report, within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

F. ***Notification of Individuals***. The Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications.

7. **Affect on lower tier transactions.** The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, regardless of whether they are for the acquisition of services, goods, or commodities. The Contractor shall incorporate the contents of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

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

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

9. **Audits and Inspections.** From time to time, DHCS may inspect the facilities, systems, books and records of the Contractor to monitor compliance with the safeguards required in the Information Confidentiality and Security Requirements (ICSR) exhibit. Contractor shall promptly remedy any violation of any provision of this ICSR exhibit. The fact that DHCS 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 ICSR exhibit.

STATE PERFORMANCE AGREEMENT: EXHIBIT E

PRIVACY AND INFORMATION SECURITY PROVISIONS

This Exhibit E 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 E consists of: (1) Protected Health Information 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 Section, Personal Information may include data provided to the Department by the Social Security Administration.

Exhibit E consists of the following parts:

1. Exhibit E-1, HIPAA Business Associate Addendum, which provides for the privacy and security of PHI.
2. Exhibit E-2, which provides for the privacy and security of PI in accordance with specified provisions of the Agreement between the Department and the Social Security Administration, known as the Information Exchange Agreement (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 E-2 further provides for the privacy and security of PI under Civil Code Section 1798.3(a) and 1798.29.
3. Exhibit E-3, Miscellaneous Provision, sets forth additional terms and conditions that extend to the provisions of Exhibit E in its entirety.

EXHIBIT E-1 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. Section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") between Department and Contractor arises only to the extent that Contractor creates, receives, maintains, transmits, uses or discloses PHI or ePHI on the Department's behalf, or provides services, arranges, performs or assists in the performance of functions or activities on behalf of the Department that are included in the definition of "business associate" in 45 C.F.R. 160.103 where the provision of the service involves the disclosure of PHI or ePHI from the Department, including but not limited to, utilization review, quality assurance, or benefit management. To the extent Contractor performs these services, functions, and activities on behalf of Department, Contractor is the Business Associate of the Department, acting on the Department's behalf. The Department and Contractor are each a party to this Agreement and are collectively referred to as the "parties."

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 E-1 of this Agreement. This information is hereafter referred to as "Department PHI".

C. The purpose of this Exhibit E-1 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 CFR Parts 160 and 164 and the HITECH Act. To the extent that data is both PHI or ePHI and Personally Identifying Information, both Exhibit E-2 (including Attachment B, the SSA Agreement between SSA, CHHS and DHCS, referred to in Exhibit E-2) and this Exhibit E-1 shall apply.

D. The terms used in this Exhibit E-1, 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.

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 E-1 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. Section 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 CFR section 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 CFR Section 160.103.

H. Privacy Rule shall mean the HIPAA Regulations that are found at 45 CFR 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 CFR Section 160.103 and as defined under HIPAA.

J. Required by law, as set forth under 45 CFR Section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

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

L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of 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 E-1 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 CFR Parts 160 and 164.

N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. Section 17932(h), any guidance issued 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 E-1, Contractor may use or disclose Department PHI only to perform functions, activities or services specified in Section 1.A of Exhibit E-1 of this Agreement, for, or on behalf of the Department, provided that such use or disclosure would not violate the HIPAA regulations or the limitations set forth in 42 CFR Part 2, or any other applicable law, 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 CFR Section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

B. Specific Use and Disclosure Provisions. Except as otherwise indicated in this Exhibit E-1, Contractor may:

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, in accordance with section D(7) of this Exhibit E-1, 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. Section 17935(a) and 45 CFR Section 164.522(a).

2) Contractor shall not directly or indirectly receive remuneration in exchange for Department PHI.

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, including but not limited to 42 CFR Part 2.

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 CFR Sections 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, implementation specifications and other requirements of 45 CFR Section 164, subpart C, in compliance with 45 CFR Section164.316. 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, Data Security Requirements;

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

6) **Reporting Unauthorized Use or Disclosure.** To report to Department any use or disclosure of Department PHI not provided for by this Exhibit E 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 with respect to such Department PHI under this Exhibit E, 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. As required by HIPAA, the HITECH Act and the HIPAA regulations, including 45 CFR Sections 164.308 and 164.314, Contractor shall incorporate, when applicable, the relevant provisions of this Exhibit E-1 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 CFR Section 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 CFR Section 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.

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. Section 17935(e) and the HIPAA regulations.

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 CFR Section 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 CFR Section 164.528 and 42 U.S.C. Section 17935(c). If Contractor maintains electronic health records for the Department as of January 1, 2009 and later, Contractor must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

12) **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 or 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 (one hour if SSA data) 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 E-1, 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.

Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the Information Protection Unit (916.445.4646, 866-866-0602) or by emailing privacyofficer@dhcs.ca.gov). 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

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.

b. **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 Information Protection Unit.

c. **Complete Report**. To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit 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 whether individual notifications and a corrective action plan are required.

d. **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 42U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary (after obtaining prior written approval of DHCS). If a breach of unsecured Department PHI involves more than 500 residents of the State of California or under its jurisdiction, Contractor shall first notify DHCS, then the Secretary of the breach immediately upon discovery of the breach. If a breach involves more than 500 California residents, Contractor shall also provide, after obtaining written prior approval of DHCS, notice to the Attorney General for the State of California, Privacy Enforcement Section. 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.

e. **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 42U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days after discovery of the breach. The Department Privacy 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.

f. **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	Information Protection Unit c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 (916) 445-4646; (866) 866- 0602 Email: privacyofficer@dhcs.ca.gov Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Service Desk (916)440-7000; (800) 579-0874 Fax: (916)440-5537

13) **Termination of Agreement.** In accordance with Section 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 E-1, it shall take the following steps:

   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 E-1 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 CFR Section 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 Contractor with the web link to the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR Section 164.520, as well as any changes to such notice. Visit the DHCS website to view the most current Notice of Privacy Practices at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/NoticeofPrivacyPractices.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 for Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Exhibit E-1, Contractor shall immediately 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. Section 17934(c).

G. Termination.

1) **Term.** The Term of this Exhibit E-1 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 CFR Section 164.504(e)(2)(ii)(J).

2) **Termination for Cause.** In accordance with 45 CFR Section 164.504(e)(1)(iii), upon the Department's knowledge of a material breach or violation of this Exhibit E-1 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 E-1 and cure is not possible.

STATE PERFORMANCE AGREEMENT: EXHIBIT E-2

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 E as Attachment B and is hereby incorporated in this Agreement.

3) Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2.

B. The purpose of this Exhibit E-2 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 E-1 of this Agreement, the HIPAA Business Associate Addendum; however, to the extent that data is both PHI or ePHI and PII, both Exhibit E-1 and this Exhibit E-2 shall apply.

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 E-2, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and 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 section 1798.29(f).

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 whose unauthorized access may trigger notification requirements under Civil Code section 1798.29. For purposes of this provision, identity shall include, but not be limited to, name, address, email address, 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 Section 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 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 E-2, 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;

   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; and

   c. If the data obtained by Contractor from DHCS includes PII, Contractor 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, which are attached as Attachment B and 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. Contractor also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Contractor 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 E-2.

5) **Contractor's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit E-2 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 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) **Confidentiality of Alcohol and Drug Abuse Patient Records.** Contractor agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

9) **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 or 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 one (1) hour by email or fax** if the data is data subject to the SSA Agreement; and **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 E-1 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 Information Protection Unit, Office of HIPAA Compliance. 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 PI or PII, 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 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 Information Security Officer.

e. **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit 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 whether individual notifications and a corrective action plan are required.

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, section 1798.29and 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 Privacy 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.

g. If Contractor has reason to believe that duplicate reporting of the same

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

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.

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 to which it is incorporated.

10) **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 E-2 and for communicating on security matters with the Department.

STATE PERFORMANCE AGREEMENT: EXHIBIT E-3

Miscellaneous Terms and Conditions Applicable to Exhibit E

1) **Disclaimer**. The Department makes no warranty or representation that compliance by Contractor with this Exhibit E, 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, PI and PII.

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

   a) Contractor does not promptly enter into negotiations to amend this Exhibit E when requested by the Department pursuant to this section; or

   b) 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 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 E 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 E 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 E shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations, and, if applicable, any other relevant state and federal laws.

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, PI and PII 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 E 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 E-1, and Section 3, Item B of Exhibit E-2, 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.** 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 E. Contractor shall promptly remedy any violation of any provision of this Exhibit E. 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 E. 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 E.

12) **Due Diligence.** Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit E and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and other applicable state and federal law, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit E.

13) **Term.** The Term of this Exhibit E-1 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 CFR Section 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 E 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.

15) **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.

16) **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.

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.

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.

17) **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.

18) **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.

19) **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 Contractors 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. 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.