AGREEMENT
BETWEEN
THE COUNTY OF TEHAMA
AND
TEHAMA COUNTY DEPARTMENT OF EDUCATION

This agreement is entered into between the County of Tehama, through its Health Services Agency ("County") and Tehama County Department of Education ("Contractor") for the purpose of providing certain student alcohol and drug prevention services and activities. It is understood that the "Friday Night Live" program is funded and administered through the County and must meet the State Department of Health Care Services Program standards and regulations governing these programs.

1. RESPONSIBILITIES OF CONTRACTOR

During the term of this agreement, Contractor shall:

- Provide services that include, but are not limited to, coordination and promotion of the "Friday Night Live" program through community action, school assemblies, sober and drug-free activities, and other county-wide events. These services shall be provided on a mutually acceptable schedule between the Contractor and County in consultation with the individual schools that wish to participate.
- Engage in programming that meets the Friday Night Live Youth Development Standards of Practice, Operating Principles and Core Components outlined at http://fridaynightlive.org/about-us/cfnip-overview/.
- Use the prevention data collection and reporting service for all Friday Night Live reporting including profiles and chapter activity.
- Follow the Friday Night Live data entry instructions for the Primary Data Quality Standards reporting service through the ECCO portal as provided by County and/or the State Department of Health Care Services.
- Complete the Program Integrity Review (PIR) biennial process requirements, as determined by State Department of Health Care Services in conjunction with the California Friday Night Live Collaborative and the California Friday Night Live Partnership. Contractors that do not meet the PIR requirements shall obtain technical assistance and

training services from County and the California Friday Night Live Partnership.

- Provide services to all eligible persons in accordance with federal and state statutes and regulations. Contractor shall assure that in planning for the provision of services, the following barriers to services are considered and addressed:
    a) Lack of education materials or other resources for the provision of services.
    b) Geographic isolation and transportation need of persons seeking services or remoteness of services.
    c) Institutional, cultural and/or ethnicity barriers.
    d) Language differences.
    e) Lack of service advocates.
    f) Failure to survey or otherwise identify the barriers to service accessibility.
    g) Needs of persons with a disability.
- Document all hours worked and submit a monthly report to County, utilizing ECCO.
- Invoice County for services rendered pursuant to the terms of this Agreement.

Unlawful Use or Unlawful Use Messages Regarding Drugs

Contractor agrees that information produced through these funds, and which pertains to drugs and alcohol-related programs, shall contain a clearly written statement that there shall be no unlawful use of drugs or alcohol associated with the program. Additionally, no aspect of a drug or alcohol-related program shall include any message on the responsible use, if the use is unlawful, of drugs or alcohol (HSC Section 11999-11999.3). By signing this agreement, Contractor agrees that it will enforce these requirements.

Restriction on Distribution of Sterile Needles

No Substance Use Prevention, Treatment, and Recovery Services Block Grant (SUPTRSBG) funds made available through this Agreement shall be used to carry out any program that includes the distribution of sterile needles or syringes for the hypodermic injection of any illegal drug unless the State Department of Health Care Services chooses to implement a demonstration syringe services program for injecting drug users.

2. **RESPONSIBILITIES OF THE COUNTY**

County shall compensate Contractor for said services pursuant to Sections 3 and 4 of this agreement. County shall monitor the Contractor's performance, quality and quantity of services performed under this agreement. The monitoring criteria shall include, but not be limited to:

- Whether the quantity of work or services being performed conforms to the Responsibilities of the Contractor section of the agreement;
- Whether the Contractor has established appropriate quality standards;
- Whether the Contractor is abiding by all the terms and requirements of the agreement;
- Whether the Contractor is abiding by programmatic and fiscal requirements;
- Whether the State Department of Health Care Services' reports have identified non-compliant services or processes which require a Corrective Action Plan ("CAP"). If a CAP is required, the Contractor, in coordination with its subcontracted provider, shall submit a CAP to the State Department of Health Care Services within the designated timeframe specified. The CAP shall be sent by secure, encrypted e-mail to SUDCountyReports@dhcs.ca.gov.

3. **COMPENSATION**

Contractor shall be paid an all-inclusive flat fee of $88,073.00 per fiscal year (July-June) for all services rendered under this agreement. Contractor shall not be entitled to payment or reimbursement for any tasks or services performed except as specified herein. Contractor shall not be paid any compensation or reimbursement beyond the flat fee amount set forth above, and Contractor agrees that County has no obligation, whatsoever, to compensate or reimburse Contractor for any expenses, direct or indirect costs, expenditures, or charges of any nature by Contractor that exceed the flat fee amount set forth above. Should Contractor receive any such payment it shall immediately notify County and shall immediately repay all such funds to County. This provision shall survive the expiration or other termination of this agreement.

4. **BILLING AND PAYMENT**

Contractor shall submit an invoice for the flat fee amount to County within thirty (30) days after service has been completed to the reasonable satisfaction of County. County shall make payment of all undisputed amounts within thirty (30) days of receipt of Contractor's invoice.

5. **TERM OF AGREEMENT**

This agreement shall commence on July 1, 2026, and shall terminate June 30, 2029, unless terminated in accordance with Section 6 below.

6. **TERMINATION OF AGREEMENT**

If Contractor fails to perform its duties to the satisfaction of the County, or if Contractor fails to fulfill in a timely and professional manner its obligations under this agreement, or if Contractor violates any of the terms or provisions of this agreement, then the County shall have the right to terminate this agreement effective immediately upon the County giving written notice thereof to the Contractor. Either party may terminate this agreement on 30 days' written notice. County shall pay contractor for all work satisfactorily completed as of the date of notice. County may terminate this agreement immediately upon oral notice should funding cease or be materially decreased or should the Tehama County Board of Supervisors fail to appropriate sufficient funds for this agreement in any fiscal year. The County's right to terminate this agreement may be exercised by the Health Services Agency Executive Director.

7. **ENTIRE AGREEMENT; MODIFICATION**

This agreement for the services specified herein supersedes all previous agreements for these services and constitutes the entire understanding between the parties hereto. Contractor shall be entitled to no other benefits other than those specified herein. No changes, amendments or alterations shall be effective unless in writing and signed by both parties. Contractor Specifically acknowledges that in entering into and executing this agreement, Contractor relies solely upon the provisions contained in this agreement and no other oral or written representation.

8. **NONASSIGNMENT OF AGREEMENT**

Inasmuch as this Agreement is intended to secure the specialized services of Contractor, Contractor may not assign, transfer, delegate, subcontract, or sublet any obligations under this Agreement, or the Agreement as a whole, without the prior written consent of the County. Notwithstanding the foregoing, Contractor may assign its rights and obligations under this Agreement, in whole but not in part, without the County's permission, in connection with any merger, consolidation, sale of all or substantially all of Contractor's assets or equity, or any other similar transaction; *provided, that* the assignee: (a) provides prompt written notice of such assignment to the non-assigning party; (b) is capable of fully performing the obligations of the Contractor under the Agreement; and (c) agrees to be bound by the terms and conditions of this Agreement. The Agreement is binding on the parties hereto and their respective successors and permitted assigns.

9. **EMPLOYMENT STATUS**

Contractor shall, during the entire term of this agreement, be construed to be an independent contractor and nothing in this agreement is intended nor shall be construed to create an employer-employee relationship, a joint venture relationship, or to allow County to exercise discretion or control over the professional manner in which Contractor performs the services which are the subject matter of this agreement; provided always, however, that the services to be provided by Contractor shall be provided in a manner consistent with the professional standards applicable to such services. The sole interest of the County is to ensure that the services shall be rendered and performed in a competent, efficient, and satisfactory manner. Contractor shall be fully responsible for payment of all taxes due to the State of California or the Federal government, which would be withheld from compensation of Contractor, if Contractor were a County employee. County shall not be liable for deductions for any amount for any purpose from Contractor's compensation. Contractor shall not be eligible for coverage under County's Workers Compensation Insurance Plan nor shall Contractor be eligible for any other County benefit.

10. **INDEMNIFICATION**

Contractor shall defend, hold harmless, and indemnify Tehama County, its elected officials, officers, employees, agents, and volunteers against all claims, suits, actions, costs, expenses (including but not limited to reasonable attorney's fees of County), damages, judgments, or decrees by reason of any person's or persons' injury, including death, or property (including property of County) being damaged, arising out of contractor's performance of work hereunder or its failure to comply with any of its obligations contained in this agreement, whether by negligence or otherwise. Contractor shall, at its own expense, defend any suit or action founded upon a claim of the foregoing. Contractor shall also defend and indemnify County against any adverse determination made by the Internal Revenue Service or the State Franchise Tax Board and/or any other taxing or regulatory agency against the County with respect to Contractor's "independent contractor" status that would establish a liability for failure to make social security or income tax withholding payments, or any other legally mandated payment.

11. **INSURANCE**

County and Contractor shall each secure and maintain in full force and effect during the full term of this agreement commercial general liability insurance or participation in a self-insurance program, including coverage for owned and non-owned automobiles and other insurance necessary to protect the public, with limits of liability of not less than $1 million combined single limit bodily injury and property damage. Policies shall be written by carriers reasonably satisfactory to each party. On request, a certificate evidencing the insurance requirements of this paragraph shall be provided.

12. **PREVAILING WAGE**

Contractor certifies that it is aware of the requirements of California Labor Code Sections 1720 et seq. and 1770 et seq., as well as California Code of Regulations, Title 8, Section 16000 et seq. ("Prevailing Wage Laws"), which require the payment of prevailing wage rates and the performance of other requirements on certain "public works" and "maintenance" projects. If the Services hereunder are being performed as part of an applicable "public works" or

"maintenance" project, as defined by the Prevailing Wage Laws, and if the total compensation is $1,000 or more, Contractor agrees to fully comply with and to require its subcontractors to fully comply with such Prevailing Wage Laws, to the extent that such laws apply. If applicable, County will maintain the general prevailing rate of per diem wages and other information set forth in Labor Code section 1773 at its principal office and will make this information available to any interested party upon request. Contractor shall defend, indemnify, and hold the County, its elected officials, officers, employees and agents free and harmless from any claims, liabilities, costs, penalties, or interest arising out of any failure or alleged failure of the Contractor or its subcontractors to comply with the Prevailing Wage Laws. Without limiting the generality of the foregoing, Contractor specifically acknowledges that County has not affirmatively represented to contractor in writing, in the call for bids, or otherwise, that the work to be covered by the bid or contract was not a "public work." To the fullest extent permitted by law, Contractor hereby specifically waives and agrees not to assert, in any manner, any past, present, or future claim for indemnification under Labor Code section 1781.

Contractor acknowledges the requirements of Labor Code sections 1725.5 and 1771.1 which provide that no contractor or subcontractor may be listed on a bid proposal or be awarded a contract for a public works project unless registered with the Department of Industrial Relations pursuant to Labor Code section 1725.5, with exceptions from this requirement specified under Labor Code sections 1725.5(f), 1771.1(a) and 1771.1(n).

If the services are being performed as part of the applicable "public works" or "maintenance" project, as defined by the Prevailing Wage Laws, Contractor acknowledges that this project is subject to compliance monitoring and enforcement by the Department of Industrial Relations.

13. **NON-DISCRIMINATION**

Contractor shall not employ discriminatory practices in the treatment of persons in relation to the circumstances provided for herein, including assignment of accommodations, employment of personnel, or in any other respect on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, sex, age, or sexual orientation.

14. GREEN PROCUREMENT POLICY

Tehama County Resolution No. 49-2002, the Green Procurement Policy (available upon request) supports recycling and waste reduction and promotes the purchase of products made with recycled materials when product fitness and quality are equal, and they are available at no more than the total cost of non-recycled products. Contractor is encouraged to conform to this policy.

15. COMPLIANCE WITH LAWS AND REGULATIONS

All services to be performed by Contractor under to this Agreement shall be performed in accordance with all applicable federal, state, and local laws, ordinances, rules, and regulations. Any change in status, licensure, or ability to perform activities, as set forth herein, must be reported to the County immediately.

16. LAW AND VENUE

This agreement shall be deemed to be made in and shall be governed by and construed in accordance with the laws of the State of California (excepting any conflict of laws provisions which would serve to defeat application of California substantive law). Venue for any action arising from this agreement shall be in Tehama County, California.

17. AUTHORITY

Each party, executing this Agreement and each person executing this Agreement in any representative capacity, hereby fully and completely warrants to all other parties that he or she has full and complete authority to bind the person or entity on whose behalf the signing party is purposing to act.

18. NOTICES

Any notice required to be given pursuant to the terms and provisions of this agreement shall be in writing and shall be sent first-class mail to the following addresses:

If to County:	Tehama County Health Services Agency Attn: Executive Director Post Office Box 400 Red Bluff, CA 96080
If to Contractor:	Tehama County Department of Education Attn: Superintendent 1135 Lincoln St. Red Bluff, CA 96080

Notice shall be deemed to be effective two days after mailing.

19. **NON-EXCLUSIVE AGREEMENT**

Contractor understands that this is not an exclusive agreement, and that County shall have the right to negotiate with and enter into agreements with others providing the same or similar services to those provided by Contractor, or to perform such services with County's own forces, as County desires.

20. **CODE OF CONDUCT**

Tehama County Health Services Agency ("County") maintains high ethical standards and is committed to complying with all applicable statutes, regulations, and guidelines. The County and each of its employees and Contractor shall follow an established Code of Conduct.

PURPOSE

The purpose of the County Code of Conduct is to ensure that all county employees and contractors are committed to conducting their activities in accordance with the highest levels of ethics and in compliance with all applicable State and Federal statutes, regulations, and guidelines. The Code of Conduct also serves to demonstrate County's dedication to providing quality care to its patients.

CODE OF CONDUCT – General Statement

- The Code of Conduct is intended to provide county employees and contractors with general guidelines to enable them to conduct the business of County in an ethical and legal manner;

- Every county employee and contractor is expected to uphold the Code of Conduct;
- Failure to comply with the Code of Conduct or failure to report non-compliance may subject the county employee or contractor to disciplinary action, up to or including termination of employment or contracted status.
- Shall perform their duties in good faith and to the best of their ability.
- Shall comply with all statutes, regulations, and guidelines applicable to Federal health care programs, and with County's own policies and procedures.
- Shall refrain from any illegal conduct. When an employee or contractor is uncertain of the meaning or application of a statute, regulation, or guideline, or the legality of a certain practice or activity, he or she shall seek guidance from his or her immediate Supervisor, Division Director, the Quality Assurance Manager, the Compliance Auditor, the Assistant Executive Director-Programs, or the Assistant Executive Director-Administration.
- Shall not obtain any improper personal benefit by virtue of their employment or contractual relationship with County;
- Shall notify their Supervisor, Division Director, Assistant Executive Director-Administration, the Assistant Executive Director-Programs, or Agency Executive Director immediately upon receipt (at work or at home) of any inquiry, subpoena, or other agency or governmental request for information regarding County;
- Shall not destroy or alter county information or documents in anticipation of, or in response to, a request for documents by any applicable governmental agency or from a court of competent jurisdiction;
- Shall not engage in any practice intended to unlawfully obtain favorable treatment or business from any entity, physician, patient, resident, vendor, or any other person or entity in a position to provide such treatment or business;
- Shall not accept any gift of more than nominal value or any hospitality or entertainment, which because of its source or value, might influence the employee's or contractors independent judgment in transactions involving County;
- Shall disclose to their Division Director any financial interest, official position, ownership interest, or any other relationship that they (or a member of their immediate family) has with county vendors or contractors;
- Shall not participate in any false billing of patients, governmental entities, or any other party;

- Shall not participate in preparation of any false cost report or other type of report submitted to the government;
- Shall not pay or arrange for County to pay any person or entity for the referral of patients to County, and shall not accept any payment or arrangement for County to accept any payment for referrals from County:
- Shall not use confidential county information for their own personal benefit or for the benefit of any other person or entity while employed at or under contract to County, or at any time thereafter;
- Shall not disclose confidential medical information pertaining to County's patients or clients without the express written consent of the patients or clients or pursuant to court order and in accordance with the applicable law and county applicable policies and procedures;
- Shall promptly report to the Quality Assurance Manager any and all violations or suspected violations of the Code of Conduct;
- Shall promptly report to the Quality Assurance Manager any and all violations or suspected violations of any statute, regulation, or guideline applicable to Federal health care programs or violations of county's own policies and procedures;
- Shall not engage in or tolerate retaliation against employees or contractors who report or suspect wrongdoing.

20. CULTURAL COMPETENCY

Contractor shall insure that services delivered under the terms of this agreement reflect a comprehensive range of age appropriate, cost-effective, high quality intervention strategies directed so as to promote wellness, avert crises, and maintain beneficiaries within their own communities. Contractor shall make every effort to deliver services which are culturally sensitive and culturally competent, and which operationalize the following values:

a. Services should be delivered in the client's primary language or language of choice since language is the primary "carrier of culture."

b. Services should encourage the active participation of individuals in their own care, protect their confidentiality at all times, and recognize the rights of all individuals regardless of race, ethnicity, cultural background, disability or personal characteristics.

c. Service delivery staff should reflect the racial, ethnic, and cultural diversity of the population being served.

d. Certain culturally sanctioned behaviors, values, or attitudes of individuals legitimately may conflict with "mainstream values" without indicating psychopathology or moral deviance.

e. Service delivery systems should reflect cultural diversity in methods of service delivery as well as policy.

f. The organization should instill values in staff which encourage them to confront racially or culturally biased behavior in themselves and others and which encourage them to increase their sensitivity and acceptance of culturally based differences.

Contractor shall adopt Culturally and Linguistically Appropriate Service ("CLAS") national standards and make every effort to deliver services which are culturally sensitive and culturally competent, and which operationalize the following CLAS Standards:

Principal Standard

Provide effective, equitable, understandable, and respectful quality care and services that are responsive to diverse cultural health beliefs and practices, preferred languages, health literacy and other communication needs.

Governance, Leadership and Workforce

- Advance and sustain organizational governance and leadership that promotes CLAS and health equity through policy, practices and allocated resources;

- Recruit, promote and support a culturally and linguistically diverse governance, leadership and workforce that are responsive to the population in the service area.

- Educate and train governance, leadership, and workforce in culturally and linguistically appropriate policies and practices on an ongoing basis.

Communication and Language Assistance

- Offer language assistance to individuals who have limited English proficiency and/or other communication needs, at no cost to them, to facilitate timely access to all health care and services.

- Inform all individuals of the availability of language assistance services clearly and in their preferred language, verbally and in writing.

- Ensure the competence of individuals providing language assistance, recognizing that the use of untrained individuals and/or minors as interpreters should be avoided.

- Provide easy-to-understand print and multimedia materials and signage in the languages commonly used by the populations in the service area.

Engagement, Continuous Improvement and Accountability

- Establish culturally and linguistically appropriate goals, policies, and management accountability, and infuse them throughout the organizations' planning and operations.

- Conduct ongoing assessments of the organization's CLAS-related activities and integrate CLAS-related measures into assessment measurement and continuous quality improvement activities.

- Collect and maintain accurate and reliable demographic data to monitor and evaluate the impact of CLAS on health equity and outcomes and to inform service delivery.

- Conduct regular assessments of community health assets and needs and use the results to plan and implement services that respond to the cultural and linguistic diversity of populations in the service area.

- Partner with the community to design, implement and evaluate policies, practices, and services to ensure cultural and linguistic appropriateness.

- Create conflict- and grievance-resolution processes that are culturally and linguistically appropriate to identify, prevent and resolve conflicts or complaints.

- Communicate the organization's progress in implementing and sustaining CLAS to all stakeholders, constituents, and the general public.

22. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Notwithstanding any other provision of this Agreement, the Contractor agrees to protect the confidentiality of any and all patient or client information with which the Contractor may come into incidental contact in the process of performing its contracted services. The Contractor shall not retain, copy, use, or disclose this information in any manner for any purpose. Violation of the confidentiality of patient or client information may, at the option of the County, be considered a material breach of this Agreement.

23. RESOLUTION OF AMBIGUITIES

If an ambiguity exists in this Agreement, or in a specific provision hereof, neither the Agreement nor the provision shall be construed against the party who drafted the Agreement or provision.

24. NO THIRD-PARTY BENEFICIARIES

Neither party intends that any person shall have a cause of action against either of them as a third-party beneficiary under this Agreement. The parties expressly acknowledge that is not their intent to create any rights or obligations in any third person or entity under this Agreement. The parties agree that this Agreement does not create, by implication or otherwise, any specific, direct or indirect obligation, duty, promise, benefit and/or special right to any person, other than the parties hereto, their successors and permitted assigns, and legal or equitable rights, remedy, or claim under or in respect to this Agreement or provisions herein.

25. TRAFFICKING VICTIMS PROTECTION ACT OF 2000

Contractor and its subcontractors that provide services covered by this agreement shall comply with the Trafficking Victims Protection Act of 2000 (22 United States Code (USC) 7104(g)) as amended by section 1702 of Pub. L. 112-239.

26. **DEBARMENT AND SUSPENSION**

County shall not subcontract with or employ any party listed on the government wide exclusions in the System for Award Management ("SAM"), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp. p. 189) and 12689 (3 CFR part 1989., p.235), "Debarment and Suspension." SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

The County shall advise all subcontractors of their obligations to comply with applicable federal debarment and suspension regulations, in addition to the requirements set forth in 42 CFR Part 1001.

If County subcontracts or employs an excluded party, DHCS has the right to withhold payments, disallow costs, or issue a CAP, as appropriate, pursuant to HSC Code 11817.8(h).

27. **STANDARDS OF THE PROFESSION**

Contractor agrees to perform its duties and responsibilities pursuant to the terms and conditions of this agreement in accordance with the standards of the profession for which Contractor has been properly licensed to practice.

28. **LICENSING OR ACCREDITATION**

Where applicable the Contractor shall maintain the appropriate license or accreditation through the life of this contract.

29. **HAZARDOUS MATERIALS**

Contractor shall provide to County all Safety Data Sheets covering all Hazardous Materials to be furnished, used, applied, or stored by Contractor, or any of its Subcontractors, in connection with the services on County property. Contractor shall provide County with copies of any such Safety Data Sheets prior to entry to County property or with a document certifying that no Hazardous Materials will be brought onto County property by Contractor, or any of its Subcontractors,

during the performance of the services. County shall provide Safety Data Sheets for any Hazardous Materials that Contractor may be exposed to while on County property.

30. **HARASSMENT**

Contractor agrees to make itself aware of and comply with the County's Harassment Policy, TCPR §8102: Harassment, which is available upon request. The County will not tolerate or condone harassment, discrimination, retaliation, or any other abusive behavior. Violations of this policy may cause termination of this agreement.

31. **COUNTERPARTS, ELECTRONIC SIGNATURES – BINDING**

This agreement may be executed in any number of counterparts, each of which will be an original, but all of which together will constitute one instrument. Each Party of this agreement agrees to the use of electronic signatures, such as digital signatures that meet the requirements of the California Uniform Electronic Transactions Act ((“CUETA”) Cal. Civil Code §§ 1633.1 to 1633.17), for executing this agreement. The Parties further agree that the electronic signatures of the Parties included in this agreement are intended to authenticate this writing and to have the same force and effect as manual signatures. Electronic signature means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record pursuant to the CUETA as amended from time to time. The CUETA authorizes use of an electronic signature for transactions and contracts among Parties in California, including a government agency. Digital signature means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature, and shall be reasonably relied upon by the Parties. For purposes of this section, a digital signature is a type of “electronic signature” as defined in subdivision (i) of Section 1633.2 of the Civil Code. Facsimile signatures or signatures transmitted via pdf document shall be treated as originals for all purposes.

32. **TRIBAL COMMUNITIES AND ORGANIZATIONS**

The Contractor shell regularly assess (e.g. review population information available through Census Bureau, compare to information obtained in CalOMS Treatment to determine whether population is being reached, survey Tribal representatives for insight in potential barriers) the

substance use service needs of the American Indian/Alaskan Native (AI/AN) population within the Contractor's geographic area and shall engage in regular and meaningful consultation and collaboration with elected officials of the tribe, Rancheria, or their designee for the purpose of identifying issues/barriers to service delivery and improvement of the quality, effectiveness, and accessibility of services available to AI/AN communities within the County.

33. NONDISCRIMINATION AND INSTITUTIONAL SAFEGUARDS FOR RELIGIOUS PROVIDERS

County shall establish such processes and procedures necessary to comply with the provisions of USC, Title 42, Section 300x-65 and CFR, Title 42, Part 54.

34. LIMITATION ON USE OF FUNDS FOR PROMOTION OF LEGALIZATION OF CONTROLLED SUBSTANCES

None of the funds made available through the Contract may be used for any activity that promotes the legalization of any drug or other substance included in Schedule I of Section 202 of the Controlled Substances Act (21 USC 812).

35. PERINATAL PRACTICE GUIDELINES

The Contractor will follow the guidelines in Document 1G, "Perinatal Practice Guideline," in developing and implementing perinatal treatment and recovery programs funded under this Exhibit, until new Perinatal Practice Guidelines are established and adopted. No formal amendment of this Contract is required for new guidelines to be incorporated into this Contract.

36. YOUTH TREATMENT GUIDELINES

The Contractor will follow the guidelines in Document 1V, "Youth Treatment Guidelines," in developing and implementing youth treatment programs funded under this Exhibit, until new Youth Treatment Guidelines are established and adopted. No formal amendment of this Contract is required for new guidelines to be incorporated into this Contract.

37. **ADDITIONAL CONTRACT REQUIREMENTS**

This Contract is subject to any additional restrictions, limitations, or conditions enacted by the Congress, or any statute enacted by the Congress, which may affect the provisions, terms, or funding of this Contract in any manner.

38. **HATCH ACT**

County agrees to comply with the provisions of the Hatch Act (USC, Title 5, Part III, Subpart F., Chapter 73, Subchapter III), which limit the political activities of employees whose principal employment activities are funded in whole or in part with federal funds.

39. **NO UNLAWFUL USE OR UNLAWFUL USE MESSAGES REGARDING DRUGS**

County agrees that information produced through these funds, and which pertains to drugs and alcohol-related programs, shall contain a clearly written statement that there shall be no unlawful use of drugs or alcohol associated with the program. Additionally, no aspect of a drug or alcohol-related program shall include any message on the responsible use, if the use is unlawful, of drugs or alcohol (HSC, Division 10.7, Chapter 1429, Sections 11999-11999.3). By signing this Enclosure, County agrees that it will enforce, and will require its subcontractors to enforce, these requirements.

40. **RESTRICTION ON DISTRIBUTION OF STERILE NEEDLES**

No SABG funds made available through this Contract shall be used to carry out any program that includes the distribution of sterile needles or syringes for the hypodermic injection of any illegal drug unless DHCS chooses to implement a demonstration syringe services program for injecting drug users.

41. **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) OF 1996**

All work performed under this Contract is subject to HIPAA, County shall perform the work in compliance with all applicable provisions of HIPAA. As identified in Exhibit E, DHCS and

County shall cooperate to assure mutual agreement as to those transactions between them, to which this provision applies. Refer to Exhibit E for additional information.

A. Trading Partner Requirements

1. No Changes. County hereby agrees that for the personal health information (Information), it will not change any definition, data condition or use of a data element or segment as proscribed in the Federal Health and Human Services (HHS) Transaction Standard Regulation (45 CFR 162.915 (a)).

2. No Additions. County hereby agrees that for the Information, it will not add any data elements or segments to the maximum data set as proscribed in the HHS Transaction Standard Regulation (45 CFR 162.915 (b)).

3. No Unauthorized Uses. County hereby agrees that for the Information, it will not use any code or data elements that either are marked "not used" in the HHS Transaction's Implementation specification or are not in the HHS Transaction Standard's implementation specifications (45 CFR 162.915 (c)).

4. No Changes to Meaning or Intent. County hereby agrees that for the Information, it will not change the meaning or intent of any of the HHS Transaction Standard's implementation specification (45 CFR 162.915 (d)).

B. Concurrence for Test Modifications to HHS Transaction Standards

County agrees and understands that there exists the possibility that DHCS or others may request an extension from the uses of a standard in the HHS Transaction Standards. If this occurs, County agrees that it will participate in such test modifications.

C. Adequate Testing

County is responsible to adequately test all business rules appropriate to their types and specialties. If the County is acting as a clearinghouse for enrolled providers, County has obligations to adequately test all business rules appropriate to each and every provider type and specialty for which they provide clearinghouse services.

D. Deficiencies

County agrees to correct transactions, errors, or deficiencies identified by DHCS, and transactions errors or deficiencies identified by an enrolled provider if the County is acting as a clearinghouse for that provider. When County is a clearinghouse, County agrees to properly communicate deficiencies and other pertinent information regarding electronic transactions to enrolled providers for which they provide clearinghouse services.

E. Code Set Retention

Both parties understand and agree to keep open code sets being processed or used in this Contract for at least the current billing period or any appeal period, whichever is longer.

F. Data Transmission Log

Both parties shall establish and maintain a Data Transmission Log which shall record any and all Data Transmissions taking place between the Parties during the term of this Contract. Each party will take necessary and reasonable steps to ensure that such Data Transmission Logs constitute a current, accurate, complete, and unaltered record of any and all Data Transmissions between the parties and shall be retained by each Party for no less than twenty-four (24) months following the date of the Data Transmission. The Data Transmission Log may be maintained on computer media or other suitable means provided that, if it is necessary to do so, the information contained in the Data Transmission Log may be retrieved in a timely manner and presented in readable form.

42. **COUNSELOR CERTIFICATION**

Any counselor or registrant providing intake, assessment of need for services, treatment, or recovery planning, individual or group counseling to participants, patients, or residents in a DHCS licensed or certified program is required to be registered or certified as defined in CCR, Title 9, Division 4, Chapter 8.

43. CULTURAL AND LINGUISTIC PROFICIENCY

To ensure equal access to quality care by diverse populations, each service provider receiving funds from this Contract shall adopt the Federal Office of Minority Health Culturally and Linguistically Appropriate Service (CLAS) national standards as outlined online at: https://minorityhealth.hhs.gov/omh/browse.aspx?lvl=2&lvlid=53https://thinkculturalhealth.hhs.gov/clas/standards.

44. INTRAVENOUS DRUG USE (IVDU) TREATMENT

County shall ensure that individuals in need of IVDU treatment shall be encouraged to undergo AOD treatment (42 USC 300x-23 (45 CFR 96.126(e)).

45. TUBERCULOSIS TREATMENT

County shall ensure the following related to Tuberculosis (TB):

A. Routinely make available TB services to individuals receiving treatment.

B. Reduce barriers to patients' accepting TB treatment.

C. Develop strategies to improve follow-up monitoring, particularly after patients leave treatment, by disseminating information through educational bulletins and technical assistance.

46. MARIJUANA RESTRICTION

Grant funds may not be used, directly or indirectly, to purchase, prescribe, or provide marijuana or treatment using marijuana. Treatment in this context includes the treatment of opioid use disorder. Grant funds also cannot be provided to any individual who or organization that provides or permits marijuana use for the purposes of treating substance use or mental disorders. See, e.g., 45 CFR. § 75.300(a) (requiring HHS to "ensure that Federal funding is expended . . . in full accordance with U.S. statutory . . . requirements."); 21 USC § 812(c) (10) and 841 (prohibiting the possession, manufacture, sale, purchase or distribution of marijuana). This prohibition does not apply to those providing such treatment in the context of clinical research

permitted by the DEA and under an FDA-approved investigational new drug application where the article being evaluated is marijuana or a constituent thereof that is otherwise a banned controlled substance under Federal law.

47. PARTICIPATION OF COUNTY BEHAVIORAL HEALTH DIRECTOR'S ASSOCIATION OF CALIFORNIA

The County AOD Program Administrator shall participate and represent the County in meetings of the County Behavioral Health Director's Association of California for the purposes of representing the counties in their relationship with DHCS with respect to policies, standards, and administration for AOD abuse services.

The County AOD Program Administrator shall attend any special meetings called by the Director of DHCS. Participation and representation shall also be provided by the County Behavioral Health Director's Association of California.

48. ADOLESCENT BEST PRACTICES GUIDELINES

County must utilize DHCS guidelines in developing and implementing youth treatment programs funded under this Enclosure The Adolescent Best Practices Guidelines can be found at: https://www.dhcs.ca.gov/Documents/CSD_CMHCS/Adol%20Best%20Practices%20Guide/AdolBestPracGuideOCTOBER2020.pdf.

49. BYRD ANTI-LOBBYING AMENDMENT (31 USC 1352)

County certifies that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 USC 1352. County shall also disclose to DHCS any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award.

50. **NONDISCRIMINATION IN EMPLOYMENT AND SERVICES**

County certifies that under the laws of the United States and the State of California, County will not unlawfully discriminate against any person.

51. **FEDERAL LAW REQUIREMENTS**

A. Title VI of the Civil Rights Act of 1964, Section 2000d, as amended, prohibiting discrimination based on race, color, or national origin in federally funded programs.

B. Title VIII of the Civil Rights Act of 1968 (42 USC 3601 et seq.) prohibiting discrimination on the basis of race, color, religion, sex, handicap, familial status or national origin in the sale or rental of housing.

C. Age Discrimination Act of 1975 (45 CFR Part 90), as amended 42 USC Sections 6101 – 6107), which prohibits discrimination on the basis of age.

D. Age Discrimination in Employment Act (29 CFR Part 1625).

E. Title I of the Americans with Disabilities Act (29 CFR Part 1630) prohibiting discrimination against the disabled in employment.

F. Title II of the Americans with Disabilities Act (28 CFR Part 35) prohibiting discrimination against the disabled by public entities.

G. Title III of the Americans with Disabilities Act (28 CFR Part 36) regarding access.

H. Section 504 of the Rehabilitation Act of 1973, as amended (29 USC Section 794), prohibiting discrimination on the basis of individuals with disabilities.

I. Executive Order 11246 (42 USC 2000(e) et seq. and 41 CFR Part 60) regarding nondiscrimination in employment under federal contracts and construction contracts greater than $10,000 funded by federal financial assistance.

J. Executive Order 13166 (67 FR 41455) to improve access to federal services for those with limited English proficiency.

K. The Drug Abuse Office and Treatment Act of 1972, as amended, relating to nondiscrimination on the basis of drug abuse.

L. Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR Part 2, Subparts A – E).

52. **STATE LAW REQUIREMENTS**

A. Fair Employment and Housing Act (Government Code Section 12900 et seq.) and the applicable regulations promulgated thereunder (2 CCR 7285.0 et seq.).

B. Title 2, Division 3, Article 9.5 of the Government Code, commencing with Section 11135.

C. Title 9, Division 4, Chapter 8 of the CCR, commencing with Section 13000.

D. No federal funds shall be used by the County or its subcontractors for sectarian worship, instruction, or proselytization. No federal funds shall be used by the County or its subcontractors to provide direct, immediate, or substantial support to any religious activity.

53. **ADDITIONAL CONTRACT RESTRICTIONS**

A. Noncompliance with the requirements of nondiscrimination in services shall constitute grounds for DHCS to withhold payments under this Contract or terminate all, or any type, of funding provided hereunder.

B. This Contract is subject to any additional restrictions, limitations, or conditions enacted by the federal or state governments that affect the provisions, terms, or funding of this Contract in any manner.

54. **SUBCONTRACT PROVISIONS**

County shall include all of the foregoing Part II general provisions in all of its subcontracts. These requirements must be included verbatim in contracts with subrecipients and not through documents incorporated by reference.

The County shall advise all subcontractors of their obligation to comply with applicable federal debarment and suspension regulations, in addition to the requirements set forth in 42 CFR Part 1001.

If a County subcontracts or employs an excluded party, DHCS has the right to withhold payments, disallow costs, or issue a CAP, as appropriate, pursuant to HSC Code 11817.8(h).

55. **INFORMATION ACCESS FOR INDIVIDUALS WITH LIMITED ENGLISH PROFICIENCY**

A. County shall comply with all applicable provisions of the Dymally-Alatorre Bilingual Services Act (Government Code sections 7290-7299.8) regarding access to materials that explain services available to the public as well as providing language interpretation services.

B. County shall comply with the applicable provisions of Section 1557 of the Affordable Care Act (45 CFR Part 92), including, but not limited to, 45 CFR 92.201, when providing access to: (a) materials explaining services available to the public, (b) language assistance, (c) language interpreter and translation services, or (d) video remote language interpreting services.

IN WITNESS WHEREOF, County and Contractor have executed this agreement on the day and year set forth below.

COUNTY OF TEHAMA

Date: _____ _____
Michelle D. Schmidt, Interim Executive Director

TEHAMA COUNTY DEPARTMENT OF EDUCATION

Date: _____ _____
Jared Caylor, Superintendent

53230
Budget Account Number

EXHIBIT A

PRIVACY AND INFORMATION SECURITY PROVISIONS

This Exhibit A 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 A 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 1798.3. Personal Information may include data provided to the Department by the Social Security Administration.

Exhibit A consists of the following parts:

1. Exhibit A-1, HIPAA Business Associate Addendum, which provides for the privacy and security of PHI.

1. Exhibit A-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 A-2 further provides for the privacy and security of PI under Civil Code Section 1798.3(a) and 1798.29.

2. Exhibit A-3, Miscellaneous Provision, sets forth additional terms and conditions that extend to the provisions of Exhibit A in its entirety.

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

C. The purpose of this Exhibit A-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 A-2 (including Attachment B, the SSA Agreement between SSA, CHHS and DHCS, referred to in Exhibit A-2) and this Exhibit A-1 shall apply.

D. The terms used in this Exhibit A-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 A-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 A-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 A-1, Contractor may use or disclose Department PHI only to perform functions, activities or services specified in Section 1.A of Exhibit A-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.

4. Specific Use and Disclosure Provisions. Except as otherwise indicated in this Exhibit A-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 A-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

5. 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 A.

6) **Reporting Unauthorized Use or Disclosure.** To report to Department any use or disclosure of Department PHI not provided for by this Exhibit A 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 A, 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 A-1 into each subcontract or sub-award 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 A-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 42 U.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
	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 A-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 A-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 A-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 A-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 A-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 A-1 and cure is not possible.

THE REST OF THIS PAGE IS INTENTIONALLY BLANK

EXHIBIT A-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 A as Attachment B and is hereby incorporated in this Agreement.

3) Title 42 Code of Federal Regulations, Chapter I, Sub-chapter A, Part 2.

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

5) **Contractor's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit A-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, Sub-chapter 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 A-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 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 which it is incorporated.

Department Program Contract	**DHCS Privacy Officer**	**DHCS Information Security Officer**
	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

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 A-2 and for communicating on security matters with the Department.

EXHIBIT A-3

Miscellaneous Terms and Conditions

Applicable to Exhibit A

1) **Disclaimer**. The Department makes no warranty or representation that compliance by Contractor with this Exhibit A, 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 A 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 A 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 A 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 A 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 A 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 A 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 A 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 A-1, and Section 3, Item B of Exhibit A-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 A. Contractor shall promptly remedy any violation of any provision of this Exhibit A. 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 A. 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 A.

12) **Due Diligence.** Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit A 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 A.

13) **Term.** The Term of this Exhibit A-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 A 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.

Attachment A
Data Security Requirements

1. Personnel Controls

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

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

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

D. **Background Check**. Before a member of the workforce may access Department PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years.

2. Technical Security Controls

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

B. **Server Security**. Servers containing unencrypted Department PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

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 revention solution.

3. Audit Controls

A. **System Security Review**. Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Department PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

B. **Log Reviews**. All systems processing and/or storing Department PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

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

4. Business Continuity / Disaster Recovery Controls

A. **Emergency Mode Operation Plan**. Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of Department PHI or PI held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

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

5. Paper Document Controls

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

B. **Escorting Visitors**. Visitors to areas where Department PHI or PI is contained shall be escorted and Department PHI or PI shall be kept out of sight while visitors are in the area.

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

D. **Removal of Data**. Only the minimum necessary Department PHI or PI may be removed from the premises of the Contractor except with express written permission of the Department. Department PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Contractor's locations to another of 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.