Yolo County Agreement No. 18-174

STATE OF CALIFORNIA
STANDARD AGREEMENT
STD 213_DHCS (Rev. 03/18)

REGISTRATION NUMBER	AGREEMENT NUMBER
	17-94627

1. This Agreement is entered into between the State Agency and the Contractor named below:

STATE AGENCY'S NAME (Also known as DHCS, CDHS, DHS or the State)
Department of Health Care Services

CONTRACTOR'S NAME (Also referred to as Contractor)
Yolo County Health and Human Services Agency

2. The term of this Agreement is: July 1, 2017 through June 30, 2022

3. The maximum amount of this Agreement is: $ 0 Zero dollars

4. The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of this Agreement.

Exhibit A – Scope Of Work	2 pages
Attachment 1 Organization And Administration	6 pages
Attachment 2 Scope Of Services	9 pages
Attachment 3 Financial Requirements	6 pages
Attachment 4 Management Information Systems	2 pages
Attachment 5 Quality Improvement System	6 pages
Attachment 6 Utilization Management Program	3 pages
Attachment 7 Access And Availability Of Services	4 pages
Attachment 8 Provider Network	11 pages

See Exhibit E, Provision 1 for additional incorporated exhibits.

Items shown above with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.
These documents can be viewed at http://www.dgs.ca.gov/ols/Resources/StandardContractLanguage.aspx.

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR

CONTRACTOR'S NAME *(if other than an individual, state whether a corporation, partnership, etc.)*
Yolo County Health & Human Services Agency

BY *(Authorized Signature)*: Oscar Villegas
DATE SIGNED *(Do not type)*: 7/24/18

PRINTED NAME AND TITLE OF PERSON SIGNING
Oscar Villegas, Yolo County Board of Supervisors, Chair

ADDRESS
137 N. Cottonwood Street, Suite 2500
Woodland, CA 95695

APPROVED AS TO FORM:
PHILIP J. POGLEDICH
COUNTY COUNSEL
By: Tyler P. Walters
DEPUTY

STATE OF CALIFORNIA

AGENCY NAME
Department of Health Care Services

BY *(Authorized Signature)*: Carrie Talbot
DATE SIGNED *(Do not type)*: 9/19/18

PRINTED NAME AND TITLE OF PERSON SIGNING
Carrie Talbot
Chief, Contract Management Unit

ADDRESS
1501 Capitol Avenue, Suite 71.2048, MS 1400, P.O. Box 997413,
Sacramento, CA 95899-7413

California Department of General Services Use Only

[X] Exempt per: W&I Code §14703

Exhibit A
SCOPE OF WORK

1. Service Overview

Contractor agrees to provide to the California Department of Health Care Services (DHCS) the services described herein.

The Contractor will provide or arrange for the provision of specialty mental health services to eligible Medi-Cal beneficiaries of Yolo County within the scope of services defined in this contract.

2. Service Location

The services shall be performed at all contracting and participating facilities of the Contractor.

3. Service Hours

The services shall be provided on a 24-hour, seven (7) days a week basis.

4. Project Representatives

A. The project representatives during the term of this contract will be:

Department of Health Care Services	**Yolo County Health and Human Services Agency**
Erika Cristo Telephone: (916) 552-9055 Fax: (916) 440-7620 Email: Erika.Cristo@dhcs.ca.gov	Karen Larsen , LMFT, Director Telephone: (530) 666-8516 Fax: (530) 666-8294 Email: klarsen@yolocounty.org

B. Direct all inquiries to:

Department of Health Care Services	**Yolo County Health and Human Services Agency**
Mental Health Services Division/Program Policy Unit Attention: Dee Taylor 1500 Capitol Avenue, MS 2702 P.O. Box Number 997413 Sacramento, CA, 95899-7413 Telephone: (916) 552-9536 Fax: (916) 440-7620 Email: Dee.Taylor@dhcs.ca.gov	Attention: Karen Larsen 137 N. Cottonwood Street, Suite 2500, Woodland, CA, 95695 Telephone: (530) 666-8516 Fax: (530) 666-8294 Email: klarsen@yolocounty.org

Exhibit A
SCOPE OF WORK

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

5. General Authority

This Contract is entered into in accordance with the Welfare and Institutions (Welf. & Inst.) Code § 14680 through §14726. Welf. & Inst. Code § 14712 directs the California Department of Health Care Services (Department) to implement and administer Managed Mental Health Care for Medi-Cal eligible residents of this state through contracts with mental health plans. The Department and Yolo County Health and Human Services Agency agrees to operate the Mental Health Plan (MHP) for Yolo County. No provision of this contract is intended to obviate or waive any requirements of applicable law or regulation, in particular, the provisions noted above. In the event a provision of this contract is open to varying interpretations, the contract provision shall be interpreted in a manner that is consistent with applicable law and regulation.

6. Americans with Disabilities Act

Contractor agrees to ensure that deliverables developed and produced, pursuant to this Agreement shall comply with the accessibility requirements of Section 508 of the Rehabilitation Act and the Americans with Disabilities Act of 1973 as amended (29 U.S.C. § 794 (d)), and regulations implementing that Act as set forth in Part 1194 of Title 36 of the Code of Federal Regulations. In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. California Government Code section 11135 codifies section 508 of the Act requiring accessibility of electronic and information technology.

7. Services to be Performed

See Exhibit A, Attachments 1 through 14 for a detailed description of the services to be performed.

Exhibit A – Attachment 1
ORGANIZATION AND ADMINISTRATION

1. Implementation Plan

The Contractor shall comply with the provisions of the Contractor's Implementation Plan as approved by the Department, including the administration of beneficiary problem resolution processes. (Cal. Code Regs., tit. 9, §§ 1810.310, 1850.205-1850.208.) The Contractor shall obtain written approval by the Department prior to making any changes to the Implementation Plan as approved by the Department. The Contractor may implement the changes if the Department does not respond in writing within thirty calendar (30) days. (Cal. Code Regs., tit. 9, § 1810.310(c)(5).)

2. Prohibited Affiliations

A. The Contractor shall not knowingly have any prohibited type of relationship with the following:

1) An individual or entity that is debarred, suspended, or otherwise excluded from participating in procurement activities under the Federal Acquisition Regulation or from participating in non-procurement activities under regulations issued under Executive Order No. 12549 or under guidelines implementing Executive Order No. 12549. (42 C.F.R. § 438.610(a)(1).)

2) An individual or entity who is an affiliate, as defined in the Federal Acquisition Regulation at 48 CFR 2.101, of a person described in this section. (42 C.F.R. § 438.610(a)(2).)

B. The Contractor shall not have a prohibited type of relationship by employing or contracting with providers or other individuals and entities excluded from participation in federal health care programs (as defined in section 1128B(f) of the Social Security Act) under either Section 1128, 1128A, 1156, or 1842(j)(2) of the Social Security Act. (42 C.F.R. §§ 438.214(d)(1), 438.610(b); 42 U.S.C. § 1320c-5.)

C. The Contractor shall not have types of relationships prohibited by this section with an excluded, debarred, or suspended individual, provider, or entity as follows:

1) A director, officer, agent, managing employee, or partner of the Contractor. (42 U.S.C. § 1320a-7(b)(8)(A)(ii); 42 C.F.R. § 438.610(c)(1).)

Exhibit A – Attachment 1
ORGANIZATION AND ADMINISTRATION

2) A subcontractor of the Contractor, as governed by 42 C.F.R. § 438.230. (42 C.F.R. § 438.610(c)(2).)

3) A person with beneficial ownership of 5 percent or more of the Contractor's equity. (42 C.F.R. § 438.610(c)(3).)

4) An individual convicted of crimes described in section 1128(b)(8)(B) of the Act. (42 C.F.R. § 438.808(b)(2).)

5) A network provider or person with an employment, consulting, or other arrangement with the Contractor for the provision of items and services that are significant and material to the Contractor's obligations under this Contract. (42 C.F.R. § 438.610(c)(4).)

6) The Contractor shall not employ or contract with, directly or indirectly, such individuals or entities for the furnishing of health care, utilization review, medical social work, administrative services, management, or provision of medical services (or the establishment of policies or provision of operational support for such services). (42 C.F.R. § 438.808(b)(3).)

D. The Contractor shall provide to the Department written disclosure of any prohibited affiliation identified by the Contractor or its subcontractors. (42 C.F.R. §438.608(c)(1).)

3. Delegation

Unless specifically prohibited by this contract or by federal or state law, Contractor may delegate duties and obligations of Contractor under this contract to subcontracting entities if Contractor determines that the subcontracting entities selected are able to perform the delegated duties in an adequate manner in compliance with the requirements of this contract. The Contractor shall maintain ultimate responsibility for adhering to and otherwise fully complying with all terms and conditions of its contract with the Department, notwithstanding any relationship(s) that the Mental Health Plan may have with any subcontractor. (42 C.F.R. § 483.230(b)(1).)

4. Subcontracts

A. This provision is a supplement to provision number five (Subcontract Requirements) in Exhibit D(F) which is attached hereto as part of this contract. As allowed by provision five in Exhibit D(F), the Department

Exhibit A – Attachment 1
ORGANIZATION AND ADMINISTRATION

hereby, and until further notice, waives its right to prior approval of subcontracts and approval of existing subcontracts.

B. No subcontract terminates the legal responsibility of the Contractor to the Department to assure that all activities under this contract are carried out. (42 C.F.R. § 230(b).)

C. All subcontracts shall be in writing.

D. All subcontracts for inpatient and residential services shall require that subcontractors maintain necessary licensing and certification or mental health program approval.

E. Each subcontract shall contain:

1) The activities and obligations, including services provided, and related reporting responsibilities. (42 C.F.R. § 438.230(c)(1)(i).)

2) The delegated activities and reporting responsibilities in compliance with the Contractor's obligations in this Contract. (42 C.F.R. § 438.230(c)(1)(ii).)

3) Subcontractor's agreement to submit reports as required by the Contractor and/or the Department.

4) The method and amount of compensation or other consideration to be received by the subcontractor from the Contractor.

5) Requirement that the subcontract be governed by, and construed in accordance with, all laws and regulations, and all contractual obligations of the Contractor under this contract.

6) Requirement that the subcontractor comply with all applicable Medicaid laws, regulations, including applicable sub-regulatory guidance and contract provisions. (42 C.F.R. § 438.230(c)(2).)

7) Terms of the subcontract including the beginning and ending dates, as well as methods for amendment and, if applicable, extension of the subcontract.

8) Provisions for full and partial revocation of the subcontract, delegated activities or obligations, or application of other remedies

Exhibit A – Attachment 1
ORGANIZATION AND ADMINISTRATION

permitted by state or federal law when the Department or the Contractor determine that the subcontractor has not performed satisfactorily. (42 C.F.R. § 438.230(c)(1)(iii).)

9) The nondiscrimination and compliance provisions of this contract as described in Exhibit E, Section 5, Paragraph C and Section 6, Paragraph C.

10) A requirement that the subcontractor make all of its premises, physical facilities, equipment, books, records, documents, contracts, computers, or other electronic systems pertaining to Medi-Cal enrollees, Medi-Cal-related activities, services and activities furnished under the terms of the subcontract, or determinations of amounts payable available at any time for inspection, examination or copying by the Department, CMS, HHS Inspector General, the United States Comptroller General, their designees, and other authorized federal and state agencies. (42 C.F.R. §438.3(h).) This audit right will exist for 10 years from the final date of the contract period or from the date of completion of any audit, whichever is later. (42 C.F.R. § 438.230(c)(3)(iii).) The Department, CMS, or the HHS Inspector General may inspect, evaluate, and audit the subcontractor at any time if there is a reasonable possibility of fraud or similar risk, then. (42 C.F.R. § 438.230(c)(3)(iv).)

11) The Department's inspection shall occur at the subcontractor's place of business, premises or physical facilities, in a form maintained in accordance with the general standards applicable to such book or record keeping, for a term of at least ten years from the close of the state fiscal year in which the subcontract was in effect. Subcontractor's agreement that assignment or delegation of the subcontract shall be void unless prior written approval is obtained from the Contractor.

12) A requirement that the Contractor monitor the subcontractor's compliance with the provisions of the subcontract and this contract and a requirement that the subcontractor provide a corrective action plan if deficiencies are identified.

Exhibit A – Attachment 1
ORGANIZATION AND ADMINISTRATION

13) Subcontractor's agreement to hold harmless both the State and beneficiaries in the event the Contractor cannot or does not pay for services performed by the subcontractor pursuant to the subcontract.

14) Subcontractor's agreement to comply with the Contractor's policies and procedures on advance directives and the Contractor's obligations for Physician Incentive Plans, if applicable based on the services provided under the subcontract.

5. Accreditation Status

A. The Contractor shall inform the Department whether it has been accredited by a private independent accrediting entity. (42 C.F.R. 438.332(a).)

B. If the Contractor has received accreditation by a private independent accrediting entity, the Contractor shall authorize the private independent accrediting entity to provide the Department a copy of its most recent accreditation review, including:

1) Its accreditation status, survey type, and level (as applicable);

2) Accreditation results, including recommended actions or improvements, corrective action plans, and summaries of findings; and

3) The expiration date of the accreditation. (42 C.F.R. § 438.332(b).)

6. Conflict of Interest

A. The Contractor shall comply with the conflict of interest safeguards described in 42 Code of Federal Regulations part 438.58 and the prohibitions described in section 1902(a)(4)(C) of the Act. (42 C.F.R. § 438.3(f)(2).)

B. Contractor's officers and employees shall not have a financial interest in this Contract or a subcontract of this Contract made by them in their official capacity, or by any body or board of which they are members unless the interest is remote. (Gov. Code §§ 1090, 1091; 42 C.F.R. § 438.3(f)(2).)

Exhibit A – Attachment 1
ORGANIZATION AND ADMINISTRATION

C. No public officials at any level of local government shall make, participate in making, or attempt to use their official positions to influence a decision made within the scope of this Contract in which they know or have reason to know that they have a financial interest. (Gov. Code §§ 87100, 87103; Cal. Code Regs., tit. 2, § 18704; 42 C.F.R. §§ 438.3(f)(2).)

1) If a public official determines not to act on a matter due to a conflict of interest within the scope of this Contract, the Contractor shall notify the Department by oral or written disclosure. (Cal. Code Regs, tit. 2, § 18707; 42 C.F.R. § 438.3(f)(2).)

2) Public officials, as defined in Government Code section 87200, shall follow the applicable requirements for disclosure of a conflict of interest or potential conflict of interest, once it is identified, and recuse themselves from discussing or otherwise acting upon the matter. (Gov. Code § 87105, Cal. Code Regs., tit. 2, § 18707(a); 42 C.F.R. § 438.3(f)(2).)

D. Contractor shall not utilize in the performance of this Contract any State officer or employee in the State civil service or other appointed State official unless the employment, activity, or enterprise is required as a condition of the officer's or employee's regular State employment. (Pub. Con. Code § 10410; 42 C.F.R. § 438.3(f)(2).)

1) Contractor shall submit documentation to the Department of employees (current and former State employees) who may present a conflict of interest.

Exhibit A – Attachment 2
SCOPE OF SERVICES

1. Provision of Services

A. The Contractor shall provide, or arrange and pay for, the following medically necessary covered Specialty Mental Health Services to beneficiaries, as defined for the purposes of this contract, of Yolo County:

1) Mental health services;

2) Medication support services;

3) Day treatment intensive;

4) Day rehabilitation;

5) Crisis intervention;

6) Crisis stabilization;

7) Adult residential treatment services;

8) Crisis residential treatment services;

9) Psychiatric health facility services;

10) Intensive Care Coordination (for beneficiaries under the age of 21);

11) Intensive Home Based Services (for beneficiaries under the age of 21);

12) Therapeutic Behavioral Services (for beneficiaries under the age of 21);

13) Therapeutic Foster Care (for beneficiaries under the age of 21);

14) Psychiatric Inpatient Hospital Services; and,

15) Targeted Case Management.

See Exhibit E, Attachment 2, Service Definitions for detailed descriptions of the SMHS listed above.

Exhibit A – Attachment 2
SCOPE OF SERVICES

B. Services shall be provided, in accordance with the State Plan, to beneficiaries, who meet medical necessity criteria, based on the beneficiary's need for services established by an assessment and documented in the client plan. Services shall be provided in an amount, duration, and scope as specified in the individualized Client Plan for each beneficiary.

C. The Contractor shall ensure that all medically necessary covered Specialty Mental Health Services are sufficient in amount, duration, or scope to reasonably achieve the purpose for which the services are furnished. The Contractor shall not arbitrarily deny or reduce the amount, duration, or scope of a medically necessary covered Specialty Mental Health Service solely because of diagnosis, type of illness, or condition of the beneficiary except as specifically provided in the medical necessity criteria applicable to the situation as provided in the California Code of Regulations, title 9, sections 1820.205, 1830.205, and 1830.210. (42 C.F.R. § 438.210(a)(2) and (3).)

D. The Contractor shall make all medically necessary covered Specialty Mental Health Services available in accordance with California Code of Regulations, title 9, sections1810.345, 1810.350 and 1810.405, and 42 Code of Federal Regulations part 438.210.

E. The Contractor shall provide second opinions from a network provider, or arrange for the beneficiary to obtain a second opinion outside the network, at no cost to the beneficiary. (42 C.F.R § 438.206(b).) At the request of a beneficiary when the Contractor or its network provider has determined that the beneficiary is not entitled to specialty mental health services due to not meeting the medical necessity criteria, the contractor shall provide for a second opinion by a licensed mental health professional (other than a psychiatric technician or a licensed vocational nurse). (Cal. Code Regs., tit. 9, § 1810.405(e).)

F. The Contractor shall provide a beneficiary's choice of the person providing services to the extent feasible in accordance with California Code of Regulations., title. 9, section1830.225 and 42 Code of Federal Regulations part 438.3(l).

G. In determining whether a service is covered under this contract based on the diagnosis of the beneficiary, the Contractor shall not exclude a beneficiary solely on the ground that the provider making the diagnosis

Exhibit A – Attachment 2
SCOPE OF SERVICES

has used the International Classification of Diseases (ICD) diagnosis system rather than the system contained in the Diagnostic and Statistical Manual (DSM) of the American Psychiatric Association.

2. Requirements for Day Treatment Intensive and Day Rehabilitation

A. The Contractor shall require providers to request payment authorization for day treatment intensive and day rehabilitation services:

1) In advance of service delivery when day treatment intensive or day rehabilitation will be provided for more than five days per week.

2) At least every three months for continuation of day treatment intensive.

3) At least every six months for continuation of day rehabilitation.

4) Contractor shall also require providers to request authorization for mental health services, as defined in California Code of Regulations, title 9, section 1810.227, provided concurrently with day treatment intensive or day rehabilitation, excluding services to treat emergency and urgent conditions as defined in California Code of Regulations, title 9, sections 1810.216 and 1810.253. These services shall be authorized with the same frequency as the concurrent day treatment intensive or day rehabilitation services.

B. The Contractor shall not delegate the payment authorization function to providers. When the Contractor is the day treatment intensive or day rehabilitation provider, the Contractor shall assure that the payment authorization function does not include staff involved in the provision of day treatment intensive, day rehabilitation services, or mental health services provided concurrent to day treatment intensive or day rehabilitation services.

C. The Contractor shall require that providers of day treatment intensive and day rehabilitation meet the requirements of California Code of Regulations, title 9, sections 1840.318, 1840.328, 1840.330, 1840.350 and 1840.352.

Exhibit A – Attachment 2
SCOPE OF SERVICES

D. The Contractor shall require that providers include, at a minimum, the following day treatment intensive and day rehabilitation service components:

1) Community meetings. These meetings shall occur at least once a day to address issues pertaining to the continuity and effectiveness of the therapeutic milieu, and shall actively involve staff and beneficiaries. Relevant discussion items include, but are not limited to: the day's schedule, any current event, individual issues that beneficiaries or staff wish to discuss to elicit support of the group and conflict resolution. Community meetings shall:

a) For day treatment intensive, include a staff person whose scope of practice includes psychotherapy.

b) For day rehabilitation, include a staff person who is a physician, a licensed/waivered/registered psychologist, clinical social worker, or marriage and family therapist; and a registered nurse, psychiatric technician, licensed vocational nurse, or mental health rehabilitation specialist.

2) Therapeutic milieu. This component must include process groups and skill-building groups. Specific activities shall be performed by identified staff and take place during the scheduled hours of operation of the program. The goal of the therapeutic milieu is to teach, model, and reinforce constructive interactions by involving beneficiaries in the overall program. For example, beneficiaries are provided with opportunities to lead community meetings and to provide feedback to peers. The program includes behavior management interventions that focus on teaching self-management skills that children, youth, adults and older adults may use to control their own lives, to deal effectively with present and future problems, and to function well with minimal or no additional therapeutic intervention. Activities include, but are not limited to, staff feedback to beneficiaries on strategies for symptom reduction, increasing adaptive behaviors, and reducing subjective distress.

3) Process groups. These groups, facilitated by staff, shall assist each beneficiary to develop necessary skills to deal with his/her

Exhibit A – Attachment 2
SCOPE OF SERVICES

problems and issues. The group process shall utilize peer interaction and feedback in developing problem-solving strategies to resolve behavioral and emotional problems. Day rehabilitation may include psychotherapy instead of process groups, or in addition to process groups.

4) Skill-building groups. In these groups, staff shall help beneficiaries identify barriers related to their psychiatric and psychological experiences. Through the course of group interaction, beneficiaries identify skills that address symptoms and increase adaptive behaviors.

5) Adjunctive therapies. These are therapies in which both staff and beneficiaries participate. These therapies may utilize self-expression, such as art, recreation, dance, or music as the therapeutic intervention. Participants do not need to have any level of skill in the area of self-expression, but rather be able utilize the modality to develop or enhance skills directed toward achieving beneficiary plan goals. Adjunctive therapies assist the beneficiary in attaining or restoring skills which enhance community functioning including problem solving, organization of thoughts and materials, and verbalization of ideas and feelings. Adjunctive therapies provided as a component of day rehabilitation or day treatment intensive are used in conjunction with other mental health services in order to improve the outcome of those services consistent with the beneficiary's needs identified in the client plan.

E. Day treatment intensive shall additionally include:

1) Psychotherapy. Psychotherapy means the use of psychological methods within a professional relationship to assist the beneficiary or beneficiaries to achieve a better psychosocial adaptation, to acquire a greater human realization of psychosocial potential and adaptation, to modify internal and external conditions that affect individual, groups, or communities in respect to behavior, emotions and thinking, in respect to their intrapersonal and interpersonal processes. Psychotherapy shall be provided by licensed, registered, or waivered staff practicing within their scope of

Exhibit A – Attachment 2
SCOPE OF SERVICES

practice. Psychotherapy does not include physiological interventions, including medication intervention.

2) Mental Health Crisis Protocol. The Contractor shall ensure that there is an established protocol for responding to beneficiaries experiencing a mental health crisis. The protocol shall assure the availability of appropriately trained and qualified staff and include agreed upon procedures for addressing crisis situations. The protocol may include referrals for crisis intervention, crisis stabilization, or other specialty mental health services necessary to address the beneficiary's urgent or emergency psychiatric condition (crisis services). If the protocol includes referrals, the day treatment intensive or day rehabilitation program staff shall have the capacity to handle the crisis until the beneficiary is linked to an outside crisis service.

3) Written Weekly Schedule. The Contractor shall ensure that a weekly detailed schedule is available to beneficiaries and as appropriate to their families, caregivers or significant support persons and identifies when and where the service components of the program will be provided and by whom. The written weekly schedule will specify the program staff, their qualifications, and the scope of their services.

F. Staffing Requirements. Staffing ratios shall be consistent with the requirements in California Code of Regulations, title 9, section 1840.350, for day treatment intensive, and California Code of Regulations section 1840.352 for day rehabilitation. For day treatment intensive, staff shall include at least one staff person whose scope of practice includes psychotherapy.

1) Program staff may be required to spend time on day treatment intensive and day rehabilitation activities outside the hours of operation and therapeutic program (e.g., time for travel, documentation, and caregiver contacts).

2) The Contractor shall require that at least one staff person be present and available to the group in the therapeutic milieu for all scheduled hours of operation.

Exhibit A – Attachment 2
SCOPE OF SERVICES

3) The Contractor shall require day treatment intensive and day rehabilitation programs to maintain documentation that enables Contractor and the Department to audit the program if it uses day treatment intensive or day rehabilitation staff who are also staff with other responsibilities (e.g., as staff of a group home, a school, or another mental health treatment program). The Contractor shall require that there is documentation of the scope of responsibilities for these staff and the specific times in which day treatment intensive or day rehabilitation activities are being performed exclusive of other activities.

G. If a beneficiary is unavoidably absent and does not attend all of the scheduled hours of the day rehabilitation or day treatment intensive program, the Contractor shall ensure that the provider receives Medi-Cal reimbursement only if the beneficiary is present for at least 50 percent of scheduled hours of operation for that day. The Contractor shall require that a separate entry be entered in the beneficiary record documenting the reason for the unavoidable absence and the total time (number of hours and minutes) the beneficiary actually attended the program that day. In cases where absences are frequent, it is the responsibility of the Contractor to ensure that the provider re-evaluates the beneficiary's need for the day rehabilitation or day treatment intensive program and takes appropriate action.

H. Documentation Standards. The Contractor shall ensure day treatment intensive and day rehabilitation documentation meets the documentation standards described in Attachment 9 of this exhibit. The documentation shall include the date(s) of service, signature of the person providing the service (or electronic equivalent), the person's type of professional degree, licensure or job title, date of signature and the total number of minutes/hours the beneficiary actually attended the program. For day treatment intensive these standards include daily progress notes on activities and a weekly clinical summary reviewed and signed by a physician, a licensed/waivered/registered psychologist, clinical social worker, or marriage and family therapist, or a registered nurse who is either staff to the day treatment intensive program or the person directing the services.

Exhibit A – Attachment 2
SCOPE OF SERVICES

I. The Contractor shall ensure that day treatment intensive and day rehabilitation have at least one contact per month with a family member, caregiver or other significant support person identified by an adult beneficiary, or one contact per month with the legally responsible adult for a beneficiary who is a minor. This contact may be face-to-face, or by an alternative method (e.g., e-mail, telephone, etc.). Adult beneficiaries may decline this service component. The contacts should focus on the role of the support person in supporting the beneficiary's community reintegration. The Contractor shall ensure that this contact occurs outside hours of operation and outside the therapeutic program for day treatment intensive and day rehabilitation.

J. Written Program Description. The Contractor shall ensure there is a written program description for day treatment intensive and day rehabilitation. The written program description must describe the specific activities of each service and reflects each of the required components of the services as described in this section. The Contractor shall review the written program description for compliance with this section with prior to the date the provider begins delivering day treatment intensive or day rehabilitation.

K. Additional higher or more specific standards. The Contractor shall retain the authority to set additional higher or more specific standards than those set forth in this contract, provided the Contractor's standards are consistent with applicable state and federal laws and regulations and do not prevent the delivery of medically necessary day treatment intensive and day rehabilitation.

L. Continuous Hours of Operation. The Contractor shall ensure that the provider applies the following when claiming for day treatment intensive and day rehabilitation services:

1) A half day shall be billed for each day in which the beneficiary receives face-to-face services in a program with services available four hours or less per day. Services must be available a minimum of three hours each day the program is open.

Exhibit A – Attachment 2
SCOPE OF SERVICES

2) A full-day shall be billed for each day in which the beneficiary receives face-to-face services in a program with services available more than four hours per day.

3) Although the beneficiary must receive face to face services on any full-day or half-day claimed, all service activities during that day are not required to be face-to-face with the beneficiary.

4) The requirement for continuous hours or operation does not preclude short breaks (for example, a school recess period) between activities. A lunch or dinner may also be appropriate depending on the program's schedule. The Contractor shall not conduct these breaks toward the total hours of operation of the day program for purposes of determining minimum hours of service.

3. Therapeutic Behavioral Services

Therapeutic Behavioral Services (TBS) are supplemental specialty mental health services covered under the Early and Periodic Screening, Diagnosis and Treatment (EPSDT) benefit as defined in California Code of Regulations section 1810.215. TBS are intensive, one-to-one services designed to help beneficiaries and their parents/caregivers manage specific behaviors using short-term measurable goals based on the beneficiary's needs. TBS are available to beneficiaries in accordance with the Department of Mental Health Information Notice 08-38, the TBS Coordination of Care Best Practices Manual, version 2 (October 2010), and the TBS Documentation Manual, version 2 (October 2009).

Exhibit A – Attachment 3
FINANCIAL REQUIREMENTS

1. Provider Compensation

The Contractor shall ensure that no payment is made to a network provider other than payment the Contractor makes for services covered under this Contract, except when these payments are specifically required to be made by the state in Title XIX of the Act, in 42 Code of Federal Regulations in chapter IV, or when the state agency makes direct payments to network providers for graduate medical education costs approved under the State Plan. (42 C.F.R. § 438.60.)

2. Payments for Indian Health Care Providers

A. Contractor shall make payment to all Indian Health Care Providers (IHCPs) in its network in a timely manner as required for payments to practitioners in individual or group practices under 42 §§ C.F.R. 447.54 and 447.46 including paying 90% of all clean claims from practitioners within 30 days of the date of receipt and paying 99 percent of all clean claims from practitioners within 90 days of the date of receipt. (42 C.F.R. 438.14(b)(2).)

B. Contractor shall pay an IHCP that is not enrolled as a FQHC, regardless of whether it is a network provider of the Contractor, its applicable encounter rate published annually in the Federal Register by the Indian Health Service or in the absence of a published encounter rate, the amount the IHPC would receive if the services were provided under the State plan's fee-for-service methodology. (42 C.F.R. § 438.14 (c)(2).)

3. Prohibited Payments

A. Federal Financial Participation is not available for any amount furnished to an excluded individual or entity, or at the direction of a physician during the period of exclusion when the person providing the service knew or had reason to know of the exclusion, or to an individual or entity when the Department failed to suspend payments during an investigation of a credible allegation of fraud. (42 U.S.C. section 1396b(i)(2).)

B. In accordance with Section 1903(i) of the Social Security Act, the Contractor is prohibited from paying for an item or service:

Exhibit A – Attachment 3
FINANCIAL REQUIREMENTS

1) Furnished under this Contract by any individual or entity during any period when the individual or entity is excluded from participation under title V, XVIII, or XX or under this title pursuant to sections 1128, 1128A, 1156, or 1842(j)(2) of the Social Security Act.

2) Furnished at the medical direction or on the prescription of a physician, during the period when such physician is excluded from participation under title V, XVIII, or XX or under this title pursuant to sections 1128, 1128A, 1156, or 1842(j)(2) of the Social Security Act and when the person furnishing such item or service knew, or had reason to know, of the exclusion (after a reasonable time period after reasonable notice has been furnished to the person).

3) Furnished by an individual or entity to whom the state has failed to suspend payments during any period when there is a pending investigation of a credible allegation of fraud against the individual or entity, unless the state determines there is good cause not to suspend such payments.

4) With respect to any amount expended for which funds may not be used under the Assisted Suicide Funding Restriction Act (ASFRA) of 1997.

4. Emergency Admission for Psychiatric Inpatient Hospital Services

The Contractor shall comply with Cal.Code Regs. Tit. 9 § 1820.225 regarding emergency admission for psychiatric inpatient hospital services regarding authorization and payment for both contract and non-contract hospitals.

5. Audit Requirements

The Contractor shall submit audited financial reports specific to this Contract on an annual basis. The audit shall be conducted in accordance with generally accepted accounting principles and generally accepted auditing standards. (42 C.F.R. § 438.3(m).)

6. Cost Reporting

A. The Contractor shall submit a fiscal year-end cost report no later than December 31 following the close of each fiscal year unless that date is

Exhibit A – Attachment 3
FINANCIAL REQUIREMENTS

extended by the Department, in accordance with the Welf. & Inst. Code § 14705(c), and/or guidelines established by the Department. Data submitted shall be full and complete and the cost report shall be certified by the Contractor's Mental Health Director and one of the following: (1) the Contractor's chief financial officer (or equivalent), (2) an individual who has delegated authority to sign for, and reports directly to, the Contractor's chief financial officer, or (3) the Contractor's auditor-controller, or equivalent. The cost report shall include both Contractor's costs and the cost of its subcontractors, if any. The cost report shall be completed in accordance with instructions contained in the Department's Cost and Financial Reporting System Instruction Manual which can be accessed through the Department's Information Technology Web Services (ITWS) for the applicable year, as well as any instructions that are incorporated by reference thereto; however, to the extent that the Contractor disagrees with such instructions, it may raise that disagreement in writing with the Department at the time the cost report is filed, and shall have the right to appeal such disagreement pursuant to procedures developed under the Welf. & Inst. Code § 14171.

B. In accordance with Welf. & Inst. Code § 5655 , the Department shall provide technical assistance and consultation to the Contractor regarding the preparation and submission of timely cost reports. If the Contractor does not submit the cost report by the reporting deadline, including any extension period granted by the Department, the Department, in accordance with Welf.& Inst. Code § 14712(e), may withhold payments of additional funds until the cost report that is due has been submitted.

C. Upon receipt of an amended cost report, which includes reconciled units of service, and a certification statement that has been signed by the Contractor's Mental Health Director and one of the following: 1) the Contractor's Chief Financial Officer (or equivalent), (2) an individual who has delegated authority to sign for, and reports directly to the Contractor's Chief Financial Officer, or (3) the county's auditor controller, or equivalent, the Department shall preliminarily settle the cost report. After completing its preliminary settlement, the Department shall so notify the Contractor if additional FFP is due to the Contractor. The Department shall submit a claim to the federal government for the related FFP within 30 days contingent upon sufficient budget authority. If funds are due to the State, the Department shall invoice the Contractor and the Contractor shall return the overpayment to the Department.

Exhibit A – Attachment 3
FINANCIAL REQUIREMENTS

7. Recovery of Overpayments

A. The Contractor, and any subcontractor or any network provider of the Contractor, shall report to the Department within 60 calendar days when it has identified payments in excess of amounts specified for reimbursement of Medicaid services. (42 C.F.R. § 438.608(c)(3).)

B. The Contractor, or subcontractor, to the extent that the subcontractor is delegated responsibility for coverage of services and payment of claims under this Contract, shall implement and maintain arrangements or procedures that include provision for the suspension of payments to a network provider for which the State, or Contractor, determines there is a credible allegation of fraud. (42 C.F.R. §§ 438.608(a)(8) and 455.23.)

C. The Contractor shall specify the retention policies for the treatment of recoveries of all overpayments from the Contractor to a provider, including specifically the retention policies for the treatment of recoveries of overpayments due to fraud, waste, or abuse. The policy shall specify the process, timeframes, and documentation required for reporting the recovery of all overpayments. The Contractor shall require its network providers to return any overpayment to the Contractor within 60 calendar days after the date on which the overpayment was identified. The Contractor shall also specify the process, timeframes, and documentation required for payment of recoveries of overpayments to the Department in situations where the Contractor is not permitted to retain some or all of the recoveries of overpayments. (42 C.F.R. § 438.608(d).)

8. Physician Incentive Plans

A. The Contractor shall obtain approval from the Department prior to implementing a Physician Incentive Plan (Cal. Code Regs. tit. 9, § 1810.438(h).).
   1) Pursuant to 42 Code of Federal Regulations part 438.3(i), the Contractor shall comply with the requirements set forth in 42 CFR §§ 422.208 and 422.210.

   2) The Contractor may operate a Physician Incentive Plan only if no specific payment can be made directly or indirectly under a Physician

Exhibit A – Attachment 3
FINANCIAL REQUIREMENTS

Incentive Plan to a physician or physician group as an inducement to reduce or limit medically necessary services furnished to a beneficiary. (42 C.F.R. § 422.(c)(1).)

3) If a physician or physician group is put at substantial financial risk for services not provided by the physician/group, the Contractor shall ensure adequate stop-loss protection to individual physicians and conduct annual beneficiary surveys. (42 C.F.R. 422.208(f).)

4) The Contractor shall provide information on its Physician Incentive Plan to any Medicaid beneficiary upon request (this includes the right to adequate and timely information on a Physician Incentive Plan). Such information shall include: whether the Contractor uses a physician incentive plan that affects the use of referral services, (2) the type of incentive arrangement, and (3) whether stop-loss protection is provided. (42 C.F.R. § 422.210(b).)

9. Beneficiary Liability for Payment

A. The Contractor or an affiliate, vendor, contractor, or subcontractor of the Contractor shall not submit a claim to, or demand or otherwise collect reimbursement from, the beneficiary or persons acting on behalf of the beneficiary for any specialty mental health or related administrative services provided under this contract, except to collect other health insurance coverage, share of cost, and co-payments. (Cal. Code Regs., tit. 9, § 1810.365 (a).)

B. The Contractor or an affiliate, vendor, contractor, or sub-subcontractor of the Contractor shall not hold beneficiaries liable for debts in the event that the Contractor becomes insolvent; for costs of covered services for which the State does not pay the Contractor; for costs of covered services for which the State or the Contractor does not pay the Contractor's network providers; for costs of covered services provided under a contract, referral or other arrangement rather than from the Contractor; or for payment of subsequent screening and treatment needed to diagnose the specific condition of or stabilize a beneficiary. 42 C.F.R. § 438.106 and Cal. Code Regs. tit 9, § 1810.365(c).)

Exhibit A – Attachment 3
FINANCIAL REQUIREMENTS

C. The Contractor shall ensure its subcontractors and providers do not bill beneficiaries, for covered services, any amount greater than would be owed if the Contractor provided the services directly (42 C.F.R. § 483.106(c).).

10. Cost Sharing

A. The Contractor shall ensure that any cost sharing imposed on beneficiaries is in accordance with 42 Code of Federal Regulations part 447.50 through 447.82. (42 C.F.R. § 438.108.)

B. The Contractor shall exempt from all cost sharing any Indian who is currently receiving or has ever received an item or service furnished by an IHCP or through referral. (42 C.F.R. § 447.56(a)(1)(x).)

11. ICD- 10

A. The Contractor shall use the criteria sets in the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5) as the clinical tool to make diagnostic determinations.

B. Once a DSM-5 diagnosis is determined, the Contractor shall determine the corresponding mental health diagnosis, in the International Classification of Diseases and Related Health Problems, Tenth Revision (ICD-10).

C. The Contractor shall use the ICD-10 diagnosis code(s) to submit a claim for specialty mental health services to receive reimbursement of Federal Financial Participation (FFP) in accordance with the covered diagnoses for reimbursement of outpatient and inpatient Medi-Cal specialty mental health services listed in Mental Health and Substance Use Disorder Services (MHSUDS) Information Notice 17-004E.

D. The lists of covered ICD-10 diagnosis codes in MHSUDS Information Notice 17-004E are subject to change and the Department may update them during the term of this contract. Changes to the lists of covered ICD-10 covered diagnoses do not require an amendment to this contract and the Department may implement these changes via Mental Health and Substance Use Disorder Services Information Notices.

Exhibit A – Attachment 4
MANAGEMENT INFORMATION SYSTEMS

1. Health Information Systems

A. The Contractor shall maintain a health information system that collects, analyzes, integrates, and reports data. (42 C.F.R. § 438.242(a); Cal. Code Regs., tit. 9, § 1810.376.) The system shall provide information on areas including, but not limited to, utilization, claims, grievances, and appeals. (42 C.F.R. § 438.242(a).) The Contractor shall comply with Section 6504(a) of the Affordable Care Act which requires that State claims processing and retrieval systems are able to collect data elements necessary to enable the mechanized claims processing and information retrieval systems in operation by the State to meet the requirements of section 1903(r)(1)(F) of the Social Security Act. (42 C.F.R. § 438.242(b)(1).)

B. The Contractor's health information system shall, at a minimum:

1) Collect data on beneficiary and provider characteristics as specified by the Department, and on services furnished to beneficiaries as specified by the Department; (42 C.F.R. § 438.242(b)(2).)

2) Ensure that data received from providers is accurate and complete by:

a. Verifying the accuracy and timeliness of reported data, including data from network providers compensated on the basis of capitation payments; (42 C.F.R. § 438.242(b)(3)(i).)

b. Screening the data for completeness, logic, and consistency; and (42 C.F.R. § 438.242(b)(3)(ii).)

c. Collecting service information in standardized formats to the extent feasible and appropriate, including secure information exchanges and technologies utilized for quality improvement and care coordination efforts. (42 C.F.R. § 438.242(b)(3)(iii).)

3) Make all collected data available to the Department and, upon request, to CMS. (42 C.F.R. § 438.242(b)(4).)

Exhibit A – Attachment 4
MANAGEMENT INFORMATION SYSTEMS

C. The Contractor's health information system is not required to collect and analyze all elements in electronic formats. (Cal. Code Regs., tit. 9, § 1810.376(c).)

2. Encounter Data

The Contractor shall submit encounter data to the Department at a frequency and level specified by the Department and CMS. (42 C.F.R. § 438.242(c)(2).) The Contractor shall ensure collection and maintenance of sufficient beneficiary encounter data to identify the provider who delivers service(s) to the beneficiary. (42 C.F.R. § 438.242(c)(1).) The Contractor shall submit all beneficiary encounter data that the Department is required to report to CMS under § 438.818. (42 C.F.R. § 438.242(c)(3).) The Contractor shall submit encounter data to the state in standardized Accredited Standards Committee (ASC) X12N 837 and National Council for Prescription Drug Programs (NCPDP) formats, and the ASC X12N 835 format as appropriate. (42 C.F.R. § 438.242(c)(4).)

3. Medi-Cal Eligibility Data System (MEDS) and MEDS Monthly Extract File (MMEF)

The Contractor shall enter into a Medi-Cal Privacy and Security Agreement (PSA) with the Department prior to obtaining access to MEDS and the MEDS monthly extract file (MMEF). The Contractor agrees to comply with the provisions as specified in the PSA. The County Mental Health Director or his or her authorized designee shall certify annually that Contractor is in compliance with the PSA agreement. Failure to comply with the terms of the agreement will result in the termination of access to MEDS and MMEF. (42 U.S.C. § 1396a(a)(7); 42 CFR § 431.300(a); 42 C.F.R. § 431.306(b); Welf. & Inst. Code § 14100.2(a).).

Exhibit A – Attachment 5
QUALITY IMPROVEMENT SYSTEM

1. Quality Assessment and Performance Improvement

A. The Contractor shall implement an ongoing comprehensive Quality Assessment and Performance Improvement (QAPI) Program for the services it furnishes to beneficiaries. (42 C.F.R. § 438.330 (a).)

B. The Contractor's QAPI Program shall improve Contractor's established outcomes through structural and operational processes and activities that are consistent with current standards of practice.

C. The Contractor shall have a written description of the QAPI Program that clearly defines the QAPI Program's structure and elements, assigns responsibility to appropriate individuals, and adopts or establishes quantitative measures to assess performance and to identify and prioritize area(s) for improvement. Contractor shall evaluate the impact and effectiveness of its QAPI Program annually and update the Program as necessary per Cal. Code Regs., tit. 9, § 1810.440(a)(6). (42 C.F.R. § 438.330(e)(2).)

D. The QAPI Program shall include collection and submission of performance measurement data required by the Department, which may include performance measures specified by CMS. The Contractor shall measure and annually report to the Department its performance, using the standard measures identified by the Department. (42 C.F.R. § 438.330 (a)(2), (b)(2), (c)(2).)

E. The Contractor shall conduct performance monitoring activities throughout the Contractor's operations. These activities shall include, but not be limited to, beneficiary and system outcomes, utilization management, utilization review, provider appeals, credentialing and monitoring, and resolution of beneficiary grievances.

F. The Contractor shall have mechanisms to detect both underutilization of services and overutilization of services. (42 C.F.R. § 438.330(b)(3).)

G. The Contractor shall implement mechanisms to assess beneficiary/family satisfaction. The Contractor shall assess beneficiary/family satisfaction by:

Exhibit A – Attachment 5
QUALITY IMPROVEMENT SYSTEM

1) Surveying beneficiary/family satisfaction with the Contractor's services at least annually;

2) Evaluating beneficiary grievances, appeals and fair hearings at least annually; and

3) Evaluating requests to change persons providing services at least annually.

4) The Contractor shall inform providers of the results of beneficiary/family satisfaction activities.

H. The Contractor shall implement mechanisms to monitor the safety and effectiveness of medication practices. The monitoring mechanism shall be under the supervision of a person licensed to prescribe or dispense prescription drugs. Monitoring shall occur at least annually.

I. The Contractor shall implement mechanisms to address meaningful clinical issues affecting beneficiaries system-wide.

J. The Contractor shall implement mechanisms to monitor appropriate and timely intervention of occurrences that raise quality of care concerns. The Contractor shall take appropriate follow-up action when such an occurrence is identified. The results of the intervention shall be evaluated by the Contractor at least annually.

K. Contractor's QAPI Program shall include Performance Improvement Projects as specified in paragraph 5.

2. Quality Improvement (QI) Work Plan

1. The Contractor shall have a Quality Improvement (QI) Work Plan covering the current contract cycle with documented annual evaluations and documented revisions as needed. The QI Work Plan shall include:

1) Evidence of the monitoring activities including, but not limited to, review of beneficiary grievances, appeals, expedited appeals, fair hearings, expedited fair hearings, provider appeals, and clinical

Exhibit A – Attachment 5
QUALITY IMPROVEMENT SYSTEM

records review as required by Cal. Code Regs., tit. 9, § 1810.440(a)(5) and 42 C.F.R. § 438.416(a);

2) Evidence that QI activities, including performance improvement projects, have contributed to meaningful improvement in clinical care and beneficiary service;

3) A description of completed and in-process QI activities, including performance improvement projects. The description shall include:

   a. Monitoring efforts for previously identified issues, including tracking issues over time;

   b. Objectives, scope, and planned QI activities for each year; and,

   c. Targeted areas of improvement or change in service delivery or program design.

4) A description of mechanisms the Contractor has implemented to assess the accessibility of services within its service delivery area. This shall include goals for responsiveness for the Contractor's 24-hour toll-free telephone number, timeliness for scheduling of routine appointments, timeliness of services for urgent conditions, and access to after-hours care; and

5) Evidence of compliance with the requirements for cultural competence and linguistic competence specified in Attachments 7 and 11.

3. Quality Improvement (QI) Committee and Program

A. The Contractor's QI program shall monitor the Contractor's service delivery system with the aim of improving the processes of providing care and better meeting the needs of its beneficiaries.

B. The Contractor shall establish a QI Committee to review the quality of specialty mental health services provided to beneficiaries. The QI Committee shall recommend policy decisions; review and evaluate the

Exhibit A – Attachment 5
QUALITY IMPROVEMENT SYSTEM

results of QI activities, including performance improvement projects; institute needed QI actions; ensure follow-up of QI processes; and document QI Committee meeting minutes regarding decisions and actions taken.

C. The QI Program shall be accountable to the Contractor's Director as described in Cal. Code Regs., tit. 9, § 1810.440(a)(1).

D. Operation of the QI program shall include substantial involvement by a licensed mental health professional. (Cal. Code. Regs., tit. 9, § 1810.440(a)(4).)

E. The QI Program shall include active participation by the Contractor's practitioners and providers, as well as beneficiaries and family members, in the planning, design and execution of the QI Program, as described in Cal. Code. Regs., tit. 9, § 1810.440(a)(2)(A-C).

F. QI activities shall include:

1) Collecting and analyzing data to measure against the goals, or prioritized areas of improvement that have been identified;

2) Identifying opportunities for improvement and deciding which opportunities to pursue;

3) Identifying relevant committees internal or external to the Contractor to ensure appropriate exchange of information with the QI Committee;

4) Obtaining input from providers, beneficiaries and family members in identifying barriers to delivery of clinical care and administrative services;

5) Designing and implementing interventions for improving performance;

6) Measuring effectiveness of the interventions;

Exhibit A – Attachment 5
QUALITY IMPROVEMENT SYSTEM

7) Incorporating successful interventions into the Contractor's operations as appropriate; and

8) Reviewing beneficiary grievances, appeals, expedited appeals, fair hearings, expedited fair hearings, provider appeals, and clinical records review as required by Cal. Code Regs., tit. 9, § 1810.440(a)(5).

4. External Quality Review

The Contractor shall undergo annual, external independent reviews of the quality, timeliness, and access to the services covered under this Contract, which are conducted pursuant to Subpart E of Part 438 of the Code of Federal Regulations. (42 C.F.R. §§ 438.350(a) and 438.320)

5. Performance Improvement Projects

A. The Contractor shall conduct a minimum of two Performance Improvement Projects (PIPs) per year, including any PIPs required by DHCS or CMS. DHCS may require additional PIPs. One PIP shall focus on a clinical area and one on a non-clinical area. (42 C.F.R. § 438.330(b)(1) and (d)(1).) Each PIP shall:

1) Be designed to achieve significant improvement, sustained over time, in health outcomes and beneficiary satisfaction;

2) Include measurement of performance using objective quality indicators;

3) Include implementation of interventions to achieve improvement in the access to and quality of care;

4) Include an evaluation of the effectiveness of the interventions based on the performance measures collected as part of the PIP; and,

5) Include planning and initiation of activities for increasing or sustaining improvement. (42 C.F.R. § 438.330(d)(2).)

Exhibit A – Attachment 5
QUALITY IMPROVEMENT SYSTEM

B. The Contractor shall report the status and results of each performance improvement project to the Department as requested, but not less than once per year. (42 C.F.R. § 438.330(d)(3).)

6. Practice Guidelines

A. The Contractor shall adopt practice guidelines. (42 C.F.R. § 438.236(b) and Cal. Code Regs., tit. 9, § 1810.326)

B. Such guidelines shall meet the following requirements:

1) They are based on valid and reliable clinical evidence or a consensus of health care professionals in the applicable field;

2) They consider the needs of the beneficiaries;

3) They are adopted in consultation with contracting health care professionals; and

4) They are reviewed and updated periodically as appropriate. (42 C.F.R. § 438.236(b).)

C. Contractor shall disseminate the guidelines to all affected providers and, upon request, to beneficiaries and potential beneficiaries. (42 C.F.R. § 438.236(c).)

D. Contractor shall take steps to assure that decisions for utilization management, beneficiary education, coverage of services, and any other areas to which the guidelines apply shall be consistent with the guidelines. (42 C.F.R. § 438.236(d)

Exhibit A – Attachment 6
UTILIZATION MANAGEMENT PROGRAM

1. Utilization Management

A. The Contractor shall operate a Utilization Management Program that is responsible for assuring that beneficiaries have appropriate access to specialty mental health services as required in California Code of Regulations, title 9, section 1810.440(b)(1)-(3).

B. The Utilization Management Program shall evaluate medical necessity, appropriateness and efficiency of services provided to Medi-Cal beneficiaries prospectively or retrospectively.

C. Compensation to individuals or entities that conduct utilization management activities must not be structured so as to provide incentives for the individual or entity to deny, limit, or discontinue medically necessary services to any beneficiary. (42 C.F.R. § 438.210(e).)

D. The Contractor may place appropriate limits on a service based on criteria applied under the State Plan, such as medical necessity and for the purpose of utilization control, provided that the services furnished are sufficient in amount, duration or scope to reasonably achieve the purpose for which the services are furnished. (42 C.F.R. § 438.210(a)(4)(i), (ii)(A).)

2. Service Authorization

A. Contractor shall implement mechanisms to assure authorization decision standards are met. The Contractor shall:

1) Have in place, and follow, written policies and procedures for processing requests for initial and continuing authorizations of services. (42 C.F.R. § 438.210(b)(1).)

2) Have mechanisms in effect to ensure consistent application of review criteria for authorization decisions, and shall consult with the requesting provider when appropriate. (42 C.F.R. § 438.210(b)(2)(i-ii).)

3) Have any decision to deny a service authorization request or to authorize a service in an amount, duration, or scope that is less than requested be made by a health care professional who has

Exhibit A – Attachment 6
UTILIZATION MANAGEMENT PROGRAM

appropriate clinical expertise in addressing the beneficiary's behavioral health needs. (42 C.F.R. § 438.210(b)(3).)

4) Notify the requesting provider, and give the beneficiary written notice of any decision by the Contractor to deny a service authorization request, or to authorize a service in an amount, duration, or scope that is less than requested. (42 C.F.R. § 438.210(c)) The beneficiary's notice shall meet the requirements in Attachment 12, Section 10, paragraph A and Section 9, paragraph I and be provided within the timeframes set forth in Attachment 12, Section 10, paragraph B and Section 9, paragraph I.

B. For standard authorization decisions, the Contractor shall provide notice as expeditiously as the beneficiary's condition requires not to exceed 14 calendar days following receipt of the request for service, with a possible extension of up to 14 additional calendar days when:

1) The beneficiary, or the provider, requests extension; or

2) The Contractor justifies (to the Department upon request) a need for additional information and how the extension is in the beneficiary's interest. (42 C.F.R. § 438.210(d)(1))

C. For cases in which a provider indicates, or the Contractor determines, that following the standard timeframe could seriously jeopardize the beneficiary's life or health or ability to attain, maintain, or regain maximum function, the Contractor shall make an expedited authorization decision and provide notice as expeditiously as the beneficiary's health condition requires and no later than 72 hours after receipt of the request for service. The Contractor may extend the 72-hour time period by up to 14 calendar days if the beneficiary requests an extension, or if the Contractor justifies (to the Department upon request) a need for additional information and how the extension is in the beneficiary's interest. (42 C.F.R. § 438.210(d)(2))

D. The Contractor shall act on an authorization request for treatment for urgent conditions within one hour of the request. (Cal. Code Regs., tit. 9, §§ 1810.253 1810.405, subd. (c)).

Exhibit A – Attachment 6
UTILIZATION MANAGEMENT PROGRAM

E. The Contractor shall not require prior authorization for an emergency admission for psychiatric inpatient hospital services, whether the admission is voluntary or involuntary. (Cal. Code Regs., tit. 9, §§ 1820.200(d) and 1820.225). The Contractor that is the MHP of the beneficiary being admitted on an emergency basis shall approve a request for payment authorization if the beneficiary meets the criteria for medical necessity and the beneficiary, due to a mental disorder, is a current danger to self or others, or immediately unable to provide for, or utilize, food, shelter or clothing. (Cal Code Regs, tit. 9 §§ 1820.205 and 1820.225).

F. The Contractor may not require prior authorization for an emergency admission to a psychiatric health facility when the beneficiary has an emergency psychiatric condition. (Cal. Code Regs., tit. 9, §§ 1810.216 and1830.245).

G. A Contractor shall authorize out of network services when a beneficiary with an emergency psychiatric condition is admitted on an emergency basis for psychiatric inpatient hospital services or psychiatric health facility services (Cal. Code Regs., tit. 9 §§ 1830.220, 1810.216, 1820.225, and 1830.245).

H. The Contractor shall define service authorization request in a manner that at least includes a beneficiary's request for the provision of a service. (42 C.F.R. § 431.201)

Exhibit A – Attachment 7
ACCESS AND AVAILABILITY OF SERVICES

1. Beneficiary Enrollment

A. Medi-Cal eligible beneficiaries are automatically enrolled in the single MHP in their county. (1915(b) waiver, § A, part I, para. A, p. 31.)

B. The Contractor shall be responsible for providing or arranging and paying for specialty mental health services for Medi-Cal eligible individuals in its county who require an assessment or meet medical necessity criteria for specialty mental health services. (Cal. Code Regs. tit. 9, §1810.228.) The Contractor shall accept these individuals in the order in which they are referred (including self-referral) without restriction (unless authorized by CMS), up to the limits set under this Contract. (42 C.F.R. § 438.3(d)(1).)

C. The Contractor shall not, on the basis of health status or need for health care services, discriminate against Medi-Cal eligible individuals in its county who require an assessment or meet medical necessity criteria for specialty mental health services. (42 C.F.R. § 438.3(d)(3).)

D. The Contractor shall not discriminate against Medi-Cal eligible individuals in its county who require an assessment or meet medical necessity criteria for specialty mental health services on the basis of race, color, national origin, sex, sexual orientation, gender identity, or disability and will not use any policy or practice that has the effect of discriminating on the basis of race, color, or national origin, sex, sexual orientation gender identity, or disability. (42 C.F.R. § 438.3(d)(4).)

2. Cultural Competence

A. The Contractor shall participate in the State's efforts to promote the delivery of services in a culturally competent manner to all beneficiaries, including those with limited English proficiency and diverse cultural and ethnic backgrounds, disabilities, and regardless of gender, sexual orientation or gender identity. (42 C.F.R. § 438.206(c)(2).)

B. The Contractor shall comply with the provisions of the Contractor's Cultural Competence Plan submitted and approved by the Department. The Contractor shall update the Cultural Competence Plan and submit these updates to the Department for review and approval annually. (Cal. Code Regs., tit. 9, § 1810.410, subds. (c)-(d).)

Exhibit A – Attachment 7
ACCESS AND AVAILABILITY OF SERVICES

3. Out-of-Network Services

A. If the Contractor's provider network is unable to provide necessary services, covered under this Contract, to a particular beneficiary, the Contractor shall adequately and timely cover the services out of network, for as long as the Contractor's provider network is unable to provide them. (42 C.F.R. § 438.206(b)(4).)

B. The Contractor shall require that out-of-network providers coordinate authorization and payment with the Contractor. The Contractor must ensure that the cost to the beneficiary for services provided out of network pursuant to an authorization is no greater than it would be if the services were furnished within the Contractor's network, consistent with California Code of Regulations., title 9, section 1810.365. (42 C.F.R. § 438.206(b)(5).)

C. Contractor shall comply with the requirements of California. Code of Regulations, title 9, section 1830.220 regarding providing beneficiaries access to out-of-network providers when a provider is available in Contractor's network.

4. Procedures for Serving Child Beneficiaries Placed Out-of-County

A. In accordance with Cal. Code Regs., tit. 9, § 1830.220, the Contractor in the child's county of origin shall provide or arrange for medically necessary specialty mental health services for children in a foster care aid code residing outside their counties of origin.

B. The Contractor shall use the standard forms issued by the Department, or the electronic equivalent of those forms generated from the Contractor's Electronic Health Record System, when a child in a foster care aid code is placed outside of his/her county of origin. The standard forms are:

1) Client Assessment,
2) Client Plan,
3) Service Authorization Request,
4) Client Assessment Update,
5) Progress Notes – Day Treatment Intensive Services,

Exhibit A – Attachment 7
ACCESS AND AVAILABILITY OF SERVICES

6) Progress Notes – Day Rehabilitation Services,
7) Organizational Provider Agreement (Standard Contract).

C. The Contractor may request an exemption from using the standard documents if the Contractor is subject to an externally placed requirement, such as a federal integrity agreement, that prevents the use of the standardized forms. The Contractor shall request this exemption from the Department in writing.

D. The Contractor shall ensure that the MHP in the child's adoptive parents' county of residence provides medically necessary specialty mental health services to a child in an Adoption Assistance Program (AAP) aid code residing outside his or her county of origin in the same way as the MHP would provide services to an in-county child for whom the MHP is listed as the county of responsibility on the Medi-Cal Eligibility Data System (MEDS).

E. The MHP in the child's legal guardians' county of residence shall provide medically necessary specialty mental health services to a child in a Kin-GAP aid code residing outside his or her county of origin in the same way that it would provide services to any other child for whom the MHP is listed as the county of responsibility in MEDS.

F. The Contractor shall comply with timelines specified in Cal. Code Regs., tit. 9, § 1830.220(b)(4)(A)(1-3), when processing or submitting authorization requests for children in a foster care, AAP, or Kinship Guardian Assistance Payment (Kin-GAP) aid code living outside his or her county of origin.

G. The Contractor shall submit changes to its procedures for serving beneficiaries placed outside their counties of origin pursuant to Welf. & Inst. Code § 14716 when those changes affect 25 percent or more of the Contractor's beneficiaries placed out of county. The Contractor's submission shall also include significant changes in the description of the Contractor's procedures for providing out-of-plan services in accordance with Cal. Code Regs., tit. 9, § 1830.220, when a beneficiary requires services or is placed in a county not covered by the Contractor's normal procedures.

Exhibit A – Attachment 7
ACCESS AND AVAILABILITY OF SERVICES

5. Indian Beneficiaries

The Contractor shall permit an Indian beneficiary who is eligible to receive services from an Indian health care provider (IHCP) participating as a network provider, to choose that IHCP as his or her provider, as long as that provider has capacity to provide the services. (42 C.F.R. § 438.14(b)(3).) The Contractor shall demonstrate it has sufficient IHCPs participating in its provider network to ensure timely access to services available under the contract from such providers for Indian beneficiaries who are eligible to receive services. (42 C.F.R. § 438.14(b)(1).) The Contractor shall permit Indian beneficiaries to obtain covered services from out- of-network IHCPs if the beneficiaries are otherwise eligible to receive such services. (42 C.F.R. § 438.14(b)(4).) The Contractor shall permit an out-of-network IHCP to refer an Indian beneficiary to a network provider. (42 C.F.R. § 438.14(b)(6).)

Exhibit A – Attachment 8
PROVIDER NETWORK

1. Enrollment and Screening

A. The Contractor shall ensure that all network providers are enrolled with the state as Medi-Cal providers consistent with the provider disclosure, screening, and enrollment requirements of 42 Code of Federal Regulations part 455, subparts B and E. (42 C.F.R. § 438.608(b).)

B. The Contractor may execute network provider agreements, pending the outcome of screening, enrollment, and revalidation, of up to 120 days but must terminate a network provider immediately upon determination that the network provider cannot be enrolled, or the expiration of one 120 day period without enrollment of the provider, and notify affected beneficiaries. (42 C.F.R. § 438.602(b)(2).)

2. Assessment of Capacity

A. The Contractor shall implement mechanisms to assess the capacity of service delivery for its beneficiaries. This includes monitoring the number, type, and geographic distribution of mental health services within the Contractor's delivery system.

B. The Contractor shall implement mechanisms to assess the accessibility of services within its service delivery area. This shall include the assessment of responsiveness of the Contractor's 24-hour toll-free telephone number, timeliness of scheduling routine appointments, timeliness of services for urgent conditions, and access to after-hours care.

3. Network Adequacy

A. The Contractor shall ensure that all services covered under this Contract are available and accessible to beneficiaries in a timely manner. 42 C.F.R. § 438.206(a)

B. Maintain and monitor a network of appropriate providers that is supported by written agreements for subcontractors and that is sufficient to provide adequate access to all services covered under this contract for all beneficiaries, including those with limited English proficiency or physical or mental disabilities. The Contractor shall ensure that network providers

Exhibit A – Attachment 8
PROVIDER NETWORK

provide physical access, reasonable accommodations, and accessible equipment for Medi-Cal beneficiaries with physical or mental disabilities. (42 C.F.R. § 438.206(b)(1) and (c)(3).)

C. The Contractor shall adhere to, in all geographic areas within the county, the time and distance standards for adult and pediatric mental health providers developed by the Department. (42 C.F.R. § 438.68(a), (b)(1)(iii), (3), 438.206(a).)

D. The Contractor may submit to the Department a request for Alternate Access Standards. The Department will evaluate requests and grant appropriate exceptions to the state developed standards.

4. Timely Access

A. Timely Access. In accordance with 42 C.F.R. § 438.206(c)(1), the Contractor shall comply with the requirements set forth in Cal. Code Cal. Code Regs., tit. 9, §1810.405, including the following:

1) Meet and require its providers to meet Department standards for timely access to care and services, taking into account the urgency of need for services.

2) Require subcontracted providers to have hours of operation during which services are provided to Medi-Cal beneficiaries that are no less than the hours of operation during which the provider offers services to non-Medi-Cal beneficiaries. If the provider only serves Medi-Cal beneficiaries, the Contractor shall require that hours of operation are comparable to the hours the provider makes available for Medi-Cal services that are not covered by the Contractor, or another Mental Health Plan.

3) Make services available to beneficiaries 24 hours a day, 7 days a week, when medically necessary.

4) Establish mechanisms to ensure that network providers comply with the timely access requirements;

5) Monitor network providers regularly to determine compliance with timely access requirements;

Exhibit A – Attachment 8
PROVIDER NETWORK

6) Take corrective action if there is a failure to comply with timely access requirements.

7) The timeliness standards specified in California Code of Regulations section 1810.405 and Welf. Inst. Code § 14717.1apply to out-of-plan services, as well as in-plan services.

5. Documentation of Network Adequacy

A. The Contractor shall give assurances to the Department and provide supporting documentation that demonstrates Contractor has the capacity to serve the expected enrollment in its service area in accordance with the network adequacy standards developed by the Department as required by departmental guidance and regulation. (42 C.F.R. § 438.207(a).)

B. The Contractor shall submit documentation to the Department, in a format specified by the Department, to demonstrate that it complies with the following requirements:

1) Offers an appropriate range of specialty services that are adequate for the anticipated number of beneficiaries for the service area.

2) Maintains a network of providers that is sufficient in number, mix, and geographic distribution to meet the needs of the anticipated number of beneficiaries in the service area. (42 C.F.R. § 438.207(b).)

C. The Contractor shall submit the documentation as specified by the Department, but no less frequently than the following:

1) At the time it enters into this Contract with the Department;

2) On an annual basis; and

3) At any time there has been a significant change, as defined by the Department, in Contractor's operations that would affect the adequacy and capacity of services, including the following:
   a) A decrease of 25 percent or more in services or providers available to beneficiaries;

Exhibit A – Attachment 8
PROVIDER NETWORK

b) Changes in benefits;

c) Changes in geographic service area;

d) Composition of or payments to Contractor's provider network; or

e) Enrollment of a new population in Contractor's county. (42 C.F.R. § 438.207(c).)

D. The Contractor shall include details regarding the change and Contractor's plans to ensure beneficiaries continue to have access to adequate services and providers.

6. Choice of Provider

The Contractor shall provide a beneficiary's choice of the person providing services to the extent possible and appropriate consistent with Cal. Code Regs., tit. 9, §1830.225 and 42 Code of Federal Regulations part 438.3(l).

7. Provider Selection

A. The Contractor shall have written policies and procedures for selection and retention of providers. (42 C.F.R. § 438.214(a).)

B. Contractor's policies and procedures for selection and retention of providers must not discriminate against particular providers that serve high-risk populations or specialize in conditions that require costly treatment. (42 C.F.R. §§ 438.12(a)(2), 438.214(c).)

C. In all subcontracts with network providers, the Contractor must follow the Department's uniform credentialing and re-credentialing policy. The Contractor must follow a documented process for credentialing and re-credentialing of network providers. (42 C.F.R. §§ 438.12(a)(2), , 438.214(b).)

D. The Contractor shall not employ or subcontract with providers excluded from participation in Federal health care programs under either section 1128 or section 1128A of the Act. (42 C.F.R. § 438.214(d).)

Exhibit A – Attachment 8
PROVIDER NETWORK

E. The Contractor may not discriminate in the selection, reimbursement, or indemnification of any provider who is acting within the scope of his or her license or certification under applicable state law, solely on the basis of that license or certification. (42 C.F.R. § 438.12(a)(1).)

F. The Contractor shall give practitioners or groups of practitioners who apply to be MHP contract providers and with whom the MHP decides not to contract written notice of the reason for a decision not to contract. (42 C.F.R. § 438.12(a)(1).)

G. Paragraphs A-F, above, may not be construed to:

1) Require the Contractor to subcontract with providers beyond the number necessary to meet the needs of its beneficiaries;

2) Preclude the Contractor from using different reimbursement amounts for different specialties or for different practitioners in the same specialty; or

3) Preclude the Contractor from establishing measures that are designed to maintain quality of services and control costs and are consistent with its responsibilities to beneficiaries. (42 C.F.R. § 438.12(b).)

H. Upon request, Contractor shall demonstrate to the Department that its providers are credentialed as required by paragraph C. (42 C.F.R. § 438.206(b)(6)

I. The Contractor shall establish individual, group and organizational provider selection criteria as provided for in Cal. Code Regs., tit. 9, § 1810.435.

J. Contractor shall only use licensed, registered, or waivered providers acting within their scope of practice for services that require a license, waiver, or registration. (Cal. Code Regs., tit. 9, § 1840.314(d).)

K. The Contractor is not located outside of the United States. (42 C.F.R. § 602(i).)

Exhibit A – Attachment 8
PROVIDER NETWORK

8. Provider Certification

A. The Contractor shall comply with California Code of Regulations, title 9, section 1810.435, in the selection of providers and shall review its providers for continued compliance with standards at least once every three years.

B. The Contractor shall comply with the provisions of 42 Code of Federal Regulations, sections parts 455.104, 455.105, 1002.203 and 1002.3, which relate to the provision of information about provider business transactions and provider ownership and control, prior to entering into a contract and during certification or re-certification of the provider.

C. "Satellite site" means a site owned, leased or operated by an organizational provider at which specialty mental health services are delivered to beneficiaries fewer than 20 hours per week, or, if located at a multiagency site at which specialty mental health services are delivered by no more than two employees or contractors of the provider.

D. The Contractor shall certify, or use another mental health plan's certification documents to certify, the organizational providers that subcontract with the Contractor to provide covered services in accordance with California Code of Regulations, title 9, section1810.435, and the requirements specified prior to the date on which the provider begins to deliver services under the contract, and once every three years after that date. The on-site review required by California Code of Regulations, title 9, section 1810.435(d), as a part of the certification process, shall be made of any site owned, leased, or operated by the provider and used to deliver covered services to beneficiaries, except that on-site review is not required for public school or satellite sites.

E. The Contractor may allow an organizational provider to begin delivering covered services to beneficiaries at a site subject to on-site review prior to the date of the on-site review, provided the site is operational and has any required fire clearances. The earliest date the provider may begin delivering covered services at a site subject to on-site review is the latest of these three (3) dates: 1) the date the provider's request for certification is received by the Department in accordance with the Contractor's certification procedures; 2) the date the site was operational; or 3) the date a required fire clearance was obtained. The Contractor shall complete any required on-site review of a provider's sites within six months of the

Exhibit A – Attachment 8
PROVIDER NETWORK

date the provider begins delivering covered services to beneficiaries at the site.

F. The Contractor may allow an organizational provider to continue delivering covered services to beneficiaries at a site subject to on-site review as part of the recertification process prior to the date of the on-site review, provided the site is operational and has any required fire clearances. The Contractor shall complete any required on-site review of a provider's sites within six months of the date the recertification of the provider is due.

G. The Contractor and/or the Department shall each verify through an on-site review that:

1) The organizational provider possesses the necessary license to operate, if applicable, and any required certification.

2) The space owned, leased or operated by the provider and used for services or staff meets local fire codes.

3) The physical plant of any site owned, leased, or operated by the provider and used for services or staff is clean, sanitary, and in good repair.

4) The organizational provider establishes and implements maintenance policies for any site owned, leased, or operated by the provider and used for services or staff to ensure the safety and well-being of beneficiaries and staff.

5) The organizational provider has a current administrative manual which includes: personnel policies and procedures, general operating procedures, service delivery policies, any required state or federal notices (DRA), and procedures for reporting unusual occurrences relating to health and safety issues.

6) The organizational provider maintains client records in a manner that meets the requirements of the Contractor, the requirements of Attachment 10; Exhibit 2, Attachment 2, Section 11 and Section 13 Paragraph B; and applicable state and federal standards.

7) The organizational provider has sufficient staff to allow the Contractor to claim federal financial participation (FFP) for the services that the organizational provider delivers to beneficiaries,

Exhibit A – Attachment 8
PROVIDER NETWORK

as described in California Code of Regulations, title 9, sections 1840.344 through 1840.358, as appropriate and applicable.

8) The organizational provider has written procedures for referring individuals to a psychiatrist when necessary, or to a physician, if a psychiatrist is not available.

9) The organizational provider's head of service, as defined California Code of Regulations, title 9, sections 622 through 630, is a licensed mental health professional or other appropriate individual as described in these sections.

10) For organizational providers that provide or store medications, the provider stores and dispenses medications in compliance with all pertinent state and federal standards. In particular:

a) All drugs obtained by prescription are labeled in compliance with federal and state laws. Prescription labels are altered only by persons legally authorized to do so.

b) Drugs intended for external use only and food stuffs are stored separately from drugs intended for internal use.

c) All drugs are stored at proper temperatures: room temperature drugs at 59-86 degrees Fahrenheit and refrigerated drugs at 36-46 degrees Fahrenheit.

d) Drugs are stored in a locked area with access limited to those medical personnel authorized to prescribe, dispense or administer medication.

e) Drugs are not retained after the expiration date. Intramuscular multi-dose vials are dated and initialed when opened.

f) A drug log is maintained to ensure the provider disposes of expired, contaminated, deteriorated and abandoned drugs in a manner consistent with state and federal laws.

g) Policies and procedures are in place for dispensing, administering and storing medications.

Exhibit A – Attachment 8
PROVIDER NETWORK

H. For organizational providers that provide day treatment intensive or day rehabilitation, the provider has a written description of the day treatment intensive and/or day rehabilitation program that complies with Attachment 2, Section 2 of this exhibit.

I. When an on-site review of an organizational provider would not otherwise be required and the provider offers day treatment intensive and/or day rehabilitation, the Contractor or the Department, as applicable, shall, at a minimum, review the provider's written program description for compliance with the requirements of Attachment 2, Section 2 of this exhibit.

J. On-site review is not required for hospital outpatient departments which are operating under the license of the hospital. Services provided by hospital outpatient departments may be provided either on the premises or off-site.

K. On-site review is not required for primary care and psychological clinics, as defined in Health and Safety Code section 1204.1 and licensed under the Health and Safety Code. Services provided by the clinics may be provided on the premises in accordance with the conditions of the clinic's license.

L. When on-site review of an organizational provider is required, the Contractor or the Department, as applicable, shall conduct an on-site review at least once every three years. Additional certification reviews of organizational providers may be conducted by the Contractor or Department, as applicable, at its discretion, if:

1) The provider makes major staffing changes.

2) The provider makes organizational and/or corporate structure changes (example: conversion to non-profit status).

3) The provider adds day treatment or medication support services when medications are administered or dispensed from the provider site.

4) There are significant changes in the physical plant of the provider site (some physical plant changes could require a new fire clearance).

Exhibit A – Attachment 8
PROVIDER NETWORK

5) There is a change of ownership or location.

6) There are complaints regarding the provider.

7) There are unusual events, accidents, or injuries requiring medical treatment for clients, staff or members of the community.

M. The Contractor shall monitor the performance of its subcontractors on an ongoing basis for compliance with the terms of this contract and shall subject the subcontractors' performance to periodic formal review, at a minimum in accordance with the recertification requirements. If the Contractor identifies deficiencies or areas for improvement, the Contractor and the subcontractor shall take corrective action.

N. In addition, Contractor may accept the certification of a provider by another Mental Health Plan, or by the Department, in order to meet the Contractor's obligations under Attachment 8, Sections 7 and 8. However, regardless of any such delegation to a subcontracting entity or acceptance of a certification by another MHP.

9. Provider Beneficiary Communications

A. The Contractor shall not prohibit nor otherwise restrict, a licensed, waivered, or registered professional, as defined in California Code of Regulations, title 9, sections 1810.223 and 1810.254, who is acting within the lawful scope of practice , from advising or advocating on behalf of a beneficiary for whom the provider is providing mental health services for any of the following:

1) The beneficiary's health status, medical care, or treatment options, including any alternative treatment that may be self-administered;

2) Information the beneficiary needs in order to decide among all relevant treatment options;

3) The risks, benefits, and consequences of receiving treatment or not receiving treatment; and

Exhibit A – Attachment 8
PROVIDER NETWORK

4) The beneficiary's right to participate in decisions regarding his or her health care, including the right to refuse treatment, and to express preferences about future treatment decisions. (42 C.F.R. § 438.102(a)(1).)

10. Provider Notifications

A. The Contractor shall inform providers and subcontractors, at the time they enter into a contract, about:

1) Beneficiary grievance, appeal, and fair hearing procedures and timeframes as specified in 42 CFR 438.400 through 42 CFR 438.424.

2) The beneficiary's right to file grievances and appeals and the requirements and timeframes for filing.

3) The availability of assistance to the beneficiary with filing grievances and appeals.

4) The beneficiary's right to request a State fair hearing after the Contractor has made a determination on an beneficiary's appeal, which is adverse to the beneficiary.

5) The beneficiary's right to request continuation of benefits that the Contractor seeks to reduce or terminate during an appeal or state fair hearing filing, if filed within the allowable timeframes, although the beneficiary may be liable for the cost of any continued benefits while the appeal or state fair hearing is pending if the final decision is adverse to the beneficiary.

Exhibit A – Attachment 9
DOCUMENTATION REQUIRMENTS

1. Documentation Standards

The Contractor shall set standards and implement processes that will support understanding of, and compliance with, documentation standards set forth in this section and any standards set by the Contractor. The Contractor may monitor performance so that the documentation of care provided will satisfy the requirements set forth below. The documentation standards for beneficiary care are minimum standards to support claims for the delivery of specialty mental health services. All standards shall be addressed in the beneficiary record; however, there is no requirement that the records have a specific document or section addressing these topics.

A. Assessment

1) The Contractor shall ensure that the following areas are included, as appropriate, as part of a comprehensive beneficiary record when an assessment has been performed. For children or certain other beneficiaries unable to provide a history, this information may be obtained from the parents/care-givers, etc.

a) Presenting Problem. The beneficiary's chief complaint, history of the presenting problem(s), including current level of functioning, relevant family history and current family information;

b) Relevant conditions and psychosocial factors affecting the beneficiary's physical health and mental health; including, as applicable, living situation, daily activities, social support, cultural and linguistic factors and history of trauma or exposure to trauma;

c) Mental Health History. Previous treatment, including providers, therapeutic modality (e.g., medications, psychosocial treatments) and response, and inpatient admissions. If possible, include information from other sources of clinical data, such as previous mental health records, and relevant psychological testing or consultation reports;

Exhibit A – Attachment 9
DOCUMENTATION REQUIRMENTS

d) Medical History. Relevant physical health conditions reported by the beneficiary or a significant support person. Include name and address of current source of medical treatment. For children and adolescents, the history must include prenatal and perinatal events and relevant/significant developmental history. If possible, include other medical information from medical records or relevant consultation reports;

e) Medications. Information about medications the beneficiary has received, or is receiving, to treat mental health and medical conditions, including duration of medical treatment. The assessment shall include documentation of the absence or presence of allergies or adverse reactions to medications, and documentation of an informed consent for medications;

f) Substance Exposure/Substance Use. Past and present use of tobacco, alcohol, caffeine, CAM (complementary and alternative medications) and over-the-counter, and illicit drugs;

g) Client Strengths. Documentation of the beneficiary's strengths in achieving client plan goals related to the beneficiary's mental health needs and functional impairments as a result of the mental health diagnosis;

h) Risks. Situations that present a risk to the beneficiary and/or others, including past or current trauma;

i) A mental status examination;

j) A complete diagnosis from the most current DSM, or a diagnosis from the most current ICD-code shall be documented, consistent with the presenting problems, history, mental status examination and/or other clinical data; and,

k) Additional clarifying formulation information, as needed.

Exhibit A – Attachment 9
DOCUMENTATION REQUIRMENTS

2) Timeliness/Frequency Standard for Assessment. The Contractor shall establish written standards for timeliness and frequency for the elements identified in item A of this section.

B. Client Plans

1) The Contractor shall ensure that Client Plans:

a) Have specific observable and/or specific quantifiable goals/treatment objectives related to the beneficiary's mental health needs and functional impairments as a result of the mental health diagnosis;

b) Identify the proposed type(s) of intervention/modality including a detailed description of the intervention to be provided;

c) Have a proposed frequency and duration of intervention(s);

d) Have interventions that focus and address the identified functional impairments as a result of the mental disorder (from Cal. Code Regs., tit. 9, § 1830.205(b)); have interventions that are consistent with the client plan goal;

e) Be consistent with the qualifying diagnoses;

f) Be signed (or electronic equivalent) by:

i. The person providing the service(s), or,

ii. A person representing a team or program providing services, or

iii. A person representing the Contractor providing services; or

iv. By one of the following as a co-signer, if the client plan is used to establish that services are provided under the

Exhibit A – Attachment 9
DOCUMENTATION REQUIRMENTS

direction of an approved category of staff, and if the signing staff is not of the approved category:

a) A physician,

b) A licensed/waivered psychologist,

c) A licensed/registered/waivered social worker,

d) A licensed/registered/waivered marriage and family therapist, or

e) A registered nurse, including but not limited to nurse practitioners, and clinical nurse specialists.

g) Include documentation of the beneficiary's participation in and agreement with the client plan, as described in Cal. Code Regs., tit. 9, § 1810.440(c)(2)(A)(B).

i. Examples of acceptable documentation include, but are not limited to, reference to the beneficiary's participation and agreement in the body of the plan, beneficiary signature on the plan, or a description of the beneficiary's participation and agreement in the client record;

ii. The beneficiary's signature or the signature of the beneficiary's legal representative is required on the client plan when:

a) The beneficiary is expected to be in long term treatment as determined by the MHP and,

b) The client plan provides that the beneficiary will be receiving more than one type of specialty mental health service;

Exhibit A – Attachment 9
DOCUMENTATION REQUIRMENTS

iii. When the beneficiary's signature or the signature of the beneficiary's legal representative is required on the client plan and the beneficiary refuses or is unavailable for signature, the client plan shall include a written explanation of the refusal or unavailability.

2) There shall be documentation in the client plan that a copy of the client plan was offered to the beneficiary.

3) The client plan shall be updated at least annually, or when there are significant changes in the beneficiary's condition.

C. Progress Notes

1) The Contractor shall ensure that progress notes describe how services provided reduced impairment, restored functioning, or prevented significant deterioration in an important area of life functioning outlined in the client plan. Items that shall be contained in the client record related to the beneficiary's progress in treatment include:

a) Timely documentation of relevant aspects of beneficiary care, including documentation of medical necessity;

b) Documentation of beneficiary encounters, including relevant clinical decisions, when decisions are made, alternative approaches for future interventions;

c) Interventions applied, beneficiary's response to the interventions and the location of the interventions;

d) The date the services were provided;

e) Documentation of referrals to community resources and other agencies, when appropriate;

f) Documentation of follow-up care, or as appropriate, a discharge summary; and

Exhibit A – Attachment 9
DOCUMENTATION REQUIRMENTS

g) The amount of time taken to provide services; and

h) The signature of the person providing the service (or electronic equivalent); the person's type of professional degree, licensure, or job title.

2) Timeliness/Frequency of Progress Notes. Progress notes shall be documented at the frequency by type of service indicated below:

a) Every Service Contact:

i. Mental Health Services;

ii. Medication Support Services;

iii. Crisis Intervention;

iv. Targeted Case Management;

b) Daily:

i. Crisis Residential;

ii. Crisis Stabilization (1x/23hr);

iii. Day Treatment Intensive; and

c) Weekly:

i. Day Treatment Intensive: a clinical summary reviewed and signed by a physician, a licensed/waivered psychologist, clinical social worker, or marriage and family therapist; or a registered nurse who is either staff to the day treatment intensive program or the person directing the service;

ii. Day Rehabilitation;

iii. Adult Residential.

Exhibit A – Attachment 9
DOCUMENTATION REQUIRMENTS

D. Other

1) All entries to the beneficiary record shall be legible.

2) All entries in the beneficiary record shall include:

   a) The date of service;

   b) The signature of the person providing the service (or electronic equivalent); the person's type of professional degree, licensure or job title; and the relevant identification number, if applicable.

   c) The date the documentation was entered in the beneficiary record.

3) The Contractor shall have a written definition of what constitutes a long term care beneficiary.

4) Contractor shall require providers to obtain and retain a written medication consent form signed by the beneficiary agreeing to the administration of psychiatric medication. This documentation shall include, but not be limited to, the reasons for taking such medications; reasonable alternative treatments available, if any; the type, range of frequency and amount, method (oral or injection), and duration of taking the medication; probable side effects; possible additional side effects which may occur to beneficiaries taking such medication beyond three (3) months; and that the consent, once given, may be withdrawn at any time by the beneficiary.

Exhibit A – Attachment 10
COORDINATION AND CONTINUITY OF CARE

A. Coordination of Care

A. The Contractor shall implement procedures to deliver care to and coordinate services for all of its beneficiaries. (42 C.F.R. § 438.208(b).) These procedures shall meet Department requirements and shall do the following:

1) Ensure that each beneficiary has an ongoing source of care appropriate to his or her needs and a person or entity formally designated as primarily responsible for coordinating the services accessed by the beneficiary. The beneficiary shall be provided information on how to contact their designated person or entity. (42 C.F.R. § 438.208(b)(1).)

2) Coordinate the services the Contractor furnishes to the beneficiary between settings of care, including appropriate discharge planning for short term and long-term hospital and institutional stays. Coordinate the services the Contractor furnishes to the beneficiary with the services the beneficiary receives from any other managed care organization, in FFS Medicaid, from community and social support providers, and other human services agencies used by its beneficiaries. (42 C.F.R. § 438.208(b)(2)(i)-(iv), Cal. Code Regs., tit. 9 § 1810.415.)

3) The Contractor shall share with the Department or other managed care entities serving the beneficiary the results of any identification and assessment of that beneficiary's needs to prevent duplication of those activities. (42 C.F.R. § 438.208(b)(4).)

4) Ensure that each provider furnishing services to beneficiaries maintains and shares, as appropriate, a beneficiary health record in accordance with professional standards. (42 C.F.R. § 438.208(b)(5).)

5) Ensure that, in the course of coordinating care, each beneficiary's privacy is protected in accordance with all federal and state privacy laws, including but not limited to 45 C.F.R. § 160 and § 164, subparts A and E, to the extent that such provisions are applicable. (42 C.F.R. § 438.208(b)(6).)

Exhibit A – Attachment 10
COORDINATION AND CONTINUITY OF CARE

B. The Contractor shall enter into a Memorandum of Understanding (MOU) with any Medi-Cal managed care plan serving the Contractor's beneficiaries. The Contractor shall notify the Department in writing if the Contractor is unable to enter into an MOU or if an MOU is terminated, providing a description of the Contractor's good faith efforts to enter into or maintain the MOU. The MHP shall monitor the effectiveness of its MOU with Medi-Cal managed care plans. (Cal. Code Regs., tit. 9, § 1810.370.)

C. The Contractor shall implement a transition of care policy that is consistent with federal requirements and complies with the Department's transition of care policy. (42 C.F.R. § 438.62(b)(1)-(2).)

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

1. Basic Requirements

A. The Contractor shall provide information in a manner and format that is easily understood and readily accessible to beneficiaries. (42 C.F.R. § 438.10(c)(1).) The Contractor shall provide all written materials for beneficiaries in easily understood language, format, and alternative formats that take into consideration the special needs of beneficiaries. (42 C.F.R. § 438.10(d)(6).) The Contractor shall inform beneficiaries that information is available in alternate formats and how to access those formats. (42 C.F.R. § 438.10.)

B. The Contractor shall provide the required information in this section to each beneficiary when first receiving Specialty Mental Health Services and upon request. (1915(b) Medi-Cal Specialty Mental Health Services Waiver, § (2), subd. (d), at p. 26., attachments 3, 4; Cal. Code Regs., tit. 9, § 1810.360(e).)

C. The Contractor shall operate a website that provides the content required in this section. (42 C.F.R. § 438.10.)

D. For consistency in the information provided to beneficiaries, the Contractor shall use the Department developed definitions for managed care terminology, including: appeal, excluded services, grievance, hospitalization, hospital outpatient care, medically necessary, network, non-participating provider, physician services, plan, preauthorization, participating provider, provider, skilled nursing care, and urgent care. (42 C.F.R. 438.10(c)(4)(i).)

E. The Contractor shall use Department developed model beneficiary handbooks and beneficiary notices that describe the transition of care policies for beneficiaries. (42 C.F.R. 438.62(b)(3).)

F. Beneficiary information required in this section may only be provided electronically by the Contractor if all of the following conditions are met:

1) The format is readily accessible;

2) The information is placed in a location on the Contractor's website that is prominent and readily accessible;

3) The information is provided in an electronic form which can be electronically retained and printed;

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

4) The information is consistent with the content and language requirements of this Attachment; and

5) The beneficiary is informed that the information is available in paper form without charge upon request and provides it upon request within 5 business days. (42 C.F.R. 438.10(c)(6).)

G. The Contractor shall have in place mechanisms to help beneficiaries and potential beneficiaries understand the requirements and benefits of the plan. (42 C.F.R. 438.10(c)(7).)

2. Information Provided to Beneficiaries

A. The Contractor shall provide information to beneficiaries and potential beneficiaries including, at a minimum, all of the following:

1) The basic features of managed care. (42 C.F.R. § 438.10(e)(2)(ii).)

2) The mandatory enrollment process. (42 C.F.R. § 438.10(e)(2)(iii).)

3) The service area covered by the Contractor. (42 C.F.R. § 438.10(e)(2)(iv).)

4) Covered benefits, including:

a. Which benefits are provided by the Contractor; and,

b. Which, if any, benefits are provided directly by the State.

5) The provider directory. (42 C.F.R. § 438.10(e)(2)(vi).)

6) Any cost-sharing that will be imposed by the Contractor consistent with the State Plan. (42 C.F.R. §§ 438.10(e)(2)(vii); State Plan § 4.18.)

7) The requirements for the Contractor to provide adequate access to covered services, including the network adequacy standards established in 42 Code of Federal Regulations part 438.68. (42 C.F.R. § 438.10(e)(2)(viii).)

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

8) The Contractor's responsibilities for coordination of care. (42 C.F.R. § 438.10(e)(2)(ix).)

9) To the extent available, quality and performance indicators for the Mental Health Plan, including beneficiary satisfaction. (42 C.F.R. § 438.10(e)(2)(x).)

B. The Contractor shall make a good faith effort to give written notice of termination of a contracted provider, within 15 calendar days after receipt or issuance of the termination notice, to each beneficiary who was seen on a regular basis by the terminated provider. (42 C.F.R. § 438.10(f)(1).)

3. Language and Format

A. The Contractor shall provide all written materials for potential beneficiaries and beneficiaries in a font size no smaller than 12 point. (42 C.F.R. 438.10(d)(6)(ii).)

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

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

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

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

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

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

4) Prevalent non-English language means a language identified as the primary language of 3,000 beneficiaries or five percent of the beneficiary population (whichever is lower) in the Contractor's service area as indicated on MEDs. (42 C.F.R. § 438.10(a), Cal. Code Regs., tit. 9, § 1810.410, subd. (a), para. (3).)

D. The Contractor shall make auxiliary aids and services available upon request and free of charge to each beneficiary. (42 C.F.R. § 438.10(d)(3)-(4).) Contractor shall also notify beneficiaries how to access these services. (42 C.F.R. § 438.10(d) (5)(ii)-(iii).)

E. The Contractor shall make oral interpretation and auxiliary aids, such as TTY/TDY and American Sign Language (ASL), available and free of charge for any language. (42 C.F.R. § 438.10(d)(2), (4)-(5).) Contractor shall notify beneficiaries that the service is available and how to access those services. (42 C.F.R. § 438.10(d)(5)(i), (iii).)

4. Handbook

A. The Contractor shall provide beneficiaries with a copy of the handbook and provider directory when the beneficiary first accesses services and thereafter upon request. (Cal. Code Regs., tit. 9, § 1810.360.)

B. The Contractor shall ensure that the handbook includes the current toll-free telephone number(s) that provides information in threshold languages and is available twenty-four hours a day, seven days a week. (Cal. Code Regs., tit. 9, § 1810.405, subd. (d).)

C. The beneficiary handbook shall include information that enables the beneficiary to understand how to effectively use the managed care program. This information shall include, at a minimum:

1) Benefits provided by the Contractor. (42 C.F.R. § 438.10(g)(2)(i).)

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

2) How and where to access any benefits provided by the Contractor, including any cost sharing, and how transportation is provided. (42 C.F.R. § 438.10(g)(2)(ii).)

a) The amount, duration, and scope of benefits available under the Contract in sufficient detail to ensure that beneficiaries understand the benefits to which they are entitled. (42 C.F.R. § 438.10(g)(2)(iii).)

b) Procedures for obtaining benefits, including any requirements for service authorizations and/or referrals for specialty care and for other benefits not furnished by the beneficiary's provider. (42 C.F.R. § 438.10(g)(2)(iv).)

c) Any restrictions on the beneficiary's freedom of choice among network providers. (42 C.F.R. § 438.10(g)(2)(vi).)

d) The extent to which, and how, beneficiaries may obtain benefits from out-of-network providers. (42 C.F.R. § 438.10(g)(2)(vii).)

e) Cost sharing, if any, consistent with the State Plan. (42 C.F.R. § 438.10(g)(2)(viii); State Plan § 4.18.)

f) Beneficiary rights and responsibilities, including the elements specified in § 438.100 as specified in Section 7 of this Attachment. (42 C.F.R. § 438.10(g)(2)(ix).)

g) The process of selecting and changing the beneficiary's provider. (42 C.F.R. § 438.10(g)(2)(x).)

h) Grievance, appeal, and fair hearing procedures and timeframes, consistent with 42 C.F.R. §§ 438.400 through 438.424, in a state-developed or state-approved description. Such information shall include:

1) The right to file grievances and appeals;

2) The requirements and timeframes for filing a grievance or appeal;

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

3) The availability of assistance in the filing process;

4) The right to request a state fair hearing after the Contractor has made a determination on a beneficiary's appeal which is adverse to the beneficiary;

5) The fact that, when requested by the beneficiary, benefits that the Contractor seeks to reduce or terminate will continue if the beneficiary files an appeal or a request for state fair hearing within the timeframes specified for filing, and that the beneficiary may, consistent with state policy, be required to pay the cost of services furnished while the appeal or state fair hearing is pending if the final decision is adverse to the beneficiary. (42 C.F.R. § 438.10(g)(2)(xi).)

i) How to exercise an advance directive, as set forth in 42 C.F.R. 438.3(j). (42 C.F.R. § 438.10(g)(2)(xii).)

j) How to access auxiliary aids and services, including additional information in in alternative formats or languages. (42 C.F.R. § 438.10(g)(2)(xiii).)

k) The Contractor's toll-free telephone number for member services, medical management, and any other unit providing services directly to beneficiaries. (42 C.F.R. § 438.10(g)(2)(xiv).)

l) Information on how to report suspected fraud or abuse. (42 C.F.R. § 438.10(g)(2)(xv).)

m) Additional information that is available upon request, includes the following:

1) Information on the structure and operation of the Contractor.

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

2) Physician incentive plans as set forth in 42 C.F.R. § 438.3(i). (42 C.F.R. § 438.10(f)(3).)

D. The Contractor shall give each beneficiary notice of any significant change (as defined by the Department) to information in the handbook at least 30 days before the intended effective date of the change. (42 C.F.R. § 438.10(g)(4).)

E. Consistent with 42 Code of Federal Regulations part 438.10(g)(3) and California Code of Regulations, title 9, section 1810.360, subdivision (e), the handbook will be considered provided if the Contractor:

1) Mails a printed copy of the information to the beneficiary's mailing address before the beneficiary first receives a specialty mental health service;

2) Mails a printed copy of the information upon the beneficiary's request to the beneficiary's mailing address;

3) Provides the information by email after obtaining the beneficiary's agreement to receive the information by email;

4) Posts the information on the Contractor's website and advises the beneficiary in paper or electronic form that the information is available on the internet and includes the applicable internet addresses, provided that beneficiaries with disabilities who cannot access this information online are provided auxiliary aids and services upon request at no cost; or,

5) Provides the information by any other method that can reasonably be expected to result in the beneficiary receiving that information. If the Contractor provides the handbook in-person when the beneficiary first receives specialty mental health services, the date and method of delivery shall be documented in the beneficiary's file.

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

5. Provider Directory

A. The Contractor shall make provider directories available in electronic and paper form, and ensure that the provider directories include:

1) Information on the category or categories of services available from each provider. (42 C.F.R. § 438.10(h)(1)(v).)

2) The names, any group affiliations, street addresses, telephone numbers, specialty, and website URLs of current contracted providers by category. (42 C.F.R. § 438.10(h)(1)(i)-(v).)

3) The cultural and linguistic capabilities of network providers, including languages (including ASL) offered by the provider or a skilled medical interpreter at the provider's office, and whether the provider has completed cultural competence training. (42 C.F.R. § 438.10(h)(1)(vii).)

4) Whether network providers' offices/facilities have accommodations for people with physical disabilities, including offices, exam room(s) and equipment. (42 C.F.R. § 438.10(h)(1)(viii).)

5) A means to identify which providers are accepting new beneficiaries. (42 C.F.R. § 438.10(h)(1)(vi).)

B. Information included in a paper provider directory shall be updated at least monthly and electronic provider directories shall be updated no later than 30 calendar days after the Contractor receives updated provider information. (42 C.F.R. § 438.10(h)(3).)

C. Provider directories shall be made available on the Contractor's website in a machine readable file and format as specified by the Secretary. (42 C.F.R. § 438.10(h)(4).)

6. Advance Directives

A. For purposes of this contract, advance directives means a written instruction, such as a living will or durable power of attorney for health care, recognized under California law, relating to the provision of health care when the individual is incapacitated. (42 C.F.R. § 489.100.)

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

B. The Contractor shall maintain written policies and procedures on advance directives, which include a description of applicable California law. (42 C.F.R. §§ and 438.3(j)(1)-(3), 422.128). Any written materials prepared by the Contractor for beneficiaries shall be updated to reflect changes in state laws governing advance directives as soon as possible, but no later than 90 days after the effective date of the change. (42 C.F.R. § 438.3(j)(4).)

C. The Contractor shall provide adult beneficiaries with the written information on advance directives. (42 C.F.R. § 438.3(j)(3).)

D. The Contractor shall not condition the provision of care or otherwise discriminate against an individual based on whether or not the individual has executed an advance directive. (42 C.F.R. §§ 422.128(b)(1)(ii)(F), 438.3(j).)

E. The Contractor shall educate staff concerning its policies and procedures on advance directives. (42 C.F.R. §§ 422.128(b)(1)(ii)(H), 438.3(j).)

7. Beneficiary Rights

A. The parties to this contract shall comply with applicable laws and regulations relating to patients' rights, including but not limited to Welfare and Institutions Code 5325, California Code of Regulations, title 9, sections 862 through 868, and 42 Code of Federal Regulations section 438.100. The Contractor shall ensure that its subcontractors comply with all applicable patients' rights laws and regulations.

B. The Contractor shall have written policies regarding the beneficiary rights specified in this section and ensure that its staff, subcontractors, and providers take those rights into account when providing services, including the right to:

1) Receive information in accordance with 42 C.F.R. § 438.10. (42 C.F.R. § 438.100(b)(2)(i).)

2) Be treated with respect and with due consideration for his or her dignity and privacy. (42 C.F.R. § 438.100(b)(2)(ii).)

Exhibit A – Attachment 11
INFORMATION REQUIREMENTS

3) Receive information on available treatment options and alternatives, presented in a manner appropriate to the beneficiary's condition and ability to understand. (42 C.F.R. § 438.100(b)(2)(iii).)

4) Participate in decisions regarding his or her health care, including the right to refuse treatment. (42 C.F.R. § 438.100(b)(2)(iv).)

5) Be free from any form of restraint or seclusion used as a means of coercion, discipline, convenience, or retaliation. (42 C.F.R. § 438.100(b)(2)(v).)

6) Request and receive a copy of his or her medical records, and to request that they be amended or corrected. (42 C.F.R. § 438.100(b)(2)(vi); 45 C.F.R. §§ 164.524,164.526.)

7) Be furnished services in accordance with 42 C.F.R. §§ 438.206 through 438.210. (42 C.F.R. § 438.100(b)(3).)

8) Freely exercise his or her rights without adversely affecting the way the, Contractor, subcontractor, or provider treats the beneficiary. (42 C.F.R. § 438.100(c).)

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

1. General Provisions

A. The Contractor shall have a grievance and appeal system in place for beneficiaries. (42 C.F.R. §§ 438.228(a), 438.402(a); Cal. Code Regs., tit. 9, § 1850.205.) The grievance and appeal system shall be implemented to handle appeals of adverse benefit determinations and grievances, and shall include processes to collect and track information about them. The Contractor's beneficiary problem resolution processes shall include:

1) A grievance process;

2) An appeal process; and,

3) An expedited appeal process. (Cal. Code Regs., tit. 9, § 1850.205(b)(1)-(b)(3).)

B. For the grievance, appeal, and expedited appeal processes, the Contractor shall comply with the following requirements:

1) The Contractor shall ensure that each beneficiary has adequate information about the Contractor's problem resolution processes by taking at least the following actions:

a) Including information describing the grievance, appeal, and expedited appeal processes in the Contractor's beneficiary booklet and providing the beneficiary handbook to beneficiaries as described in Attachment 11 of this contract. (Cal. Code Regs., tit. 9, § 1850.205(c)(1)(A).)

b) Posting notices explaining grievance, appeal, and expedited appeal process procedures in locations at all Contractor provider sites. Notices shall be sufficient to ensure that the information is readily available to both beneficiaries and provider staff. The posted notice shall also explain the availability of fair hearings after the exhaustion of an appeal or expedited appeal process, including information that a fair hearing may be requested whether or not the beneficiary has received a notice of adverse benefit determination. For the purposes of this Section, a Contractor provider site means

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

any office or facility owned or operated by the Contractor or a provider contracting with the Contractor at which beneficiaries may obtain specialty mental health services. (Cal. Code Regs., tit. 9, §§ 1850.205(c)(1)(B) and 1850.210.)

c) Make available forms that may be used to file grievances, appeals, and expedited appeals and self-addressed envelopes that beneficiaries can access at all Contractor provider sites without having to make a verbal or written request to anyone. (Cal. Code Regs., tit. 9, § 1850.205(c)(1)(C).)

d) Give beneficiaries any reasonable assistance in completing the forms and other procedural steps related to a grievance or appeal. This includes, but is not limited to, providing interpreter services and toll-free numbers with TTY/TDD and interpreter capability. (42 C.F.R. § 438.406(a); 42 C.F.R. § 438.228(a).)

2) The Contractor shall allow beneficiaries to file grievances and request appeals. (42 C.F.R. § 438.402(c)(1).) The Contractor shall have only one level of appeal for beneficiaries. (42 C.F.R. § 438.402(b); 42 C.F.R. § 438.228(a).)

3) A beneficiary may request a State fair hearing after receiving notice under 438.408 that the adverse benefit determination is upheld. (42 C.F.R. § 438.402(c)(1); 42 C.F.R. § 438.408(f).)

4) The Contractor shall adhere to the notice and timing requirements in §438.408. If the Contractor fails to adhere to these notice and timing requirements, the beneficiary is deemed to have exhausted the Contractor's appeals process and may initiate a State fair hearing. (42 C.F.R. §§ 438.402(c)(1)(i)(A), 438.408(c)(3).)

5) The Contractor shall acknowledge receipt of each grievance, appeal, and request for expedited appeal of adverse benefit determinations to the beneficiary in writing. (42 C.F.R. § 438.406(b)(1); 42 C.F.R. § 438.228(a); Cal. Code Regs., tit. 9, § 1850.205(d)(4).)

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

6) The Contractor shall allow a provider, or authorized representative, acting on behalf of the beneficiary and with the beneficiary's written consent to request an appeal, file a grievance, or request a state fair hearing. (42 C.F.R. § 438.402(c)(1)(i)-(ii); Cal. Code Regs., tit. 9, § 1850.205(c)(2).)

7) The Contractor shall allow a beneficiary's authorized representative to use the grievance, appeal, or expedited appeal processes on the beneficiary's behalf. (Cal. Code Regs., tit. 9, § 1850.205(c)(2).)

8) At the beneficiary's request, the Contractor shall identify staff or another individual, such as a legal guardian, to be responsible for assisting a beneficiary with these processes, including providing assistance in writing the grievance, appeal, or expedited appeal. If the individual identified by the Contractor is the person providing specialty mental health services to the beneficiary requesting assistance, the Contractor shall identify another individual to assist that beneficiary. (Cal. Code Regs., tit. 9, § 1850.205(c)(4).) Assistance includes, but is not limited to, auxiliary aids and services upon request, such as providing interpreter services and toll-free numbers with TTY/TDD and interpreter capability. (42 C.F.R. § 438.406(a).)

9) The Contractor shall not subject a beneficiary to discrimination or any other penalty for filing a grievance, appeal, or expedited appeal. (Cal. Code Regs., tit. 9, § 1850.205(c)(5).)

10) The Contractor's procedures for the beneficiary problem resolution processes shall maintain the confidentiality of each beneficiary's information. (Cal. Code Regs., tit. 9, § 1850.205(c)(6).)

11) The Contractor shall include a procedure to transmit issues identified as a result of the grievance, appeal or expedited appeal processes to the Contractor's Quality Improvement Committee, the Contractor's administration or another appropriate body within the Contractor's operations. The Contractor shall consider these issues in the Contractor's Quality Improvement Program, as required by

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

Cal. Code Regs., tit. 9, §1810.440(a)(5). (Cal. Code Regs., tit. 9, § 1850.205(c)(7).)

12) The Contractor shall ensure that decision makers on grievances and appeals of adverse benefit determinations were not involved in any previous level of review or decision-making, and were not subordinates of any individual who was involved in a previous level of review or decision-making. (42 C.F.R. § 438.406(b)(2)(i); 42 C.F.R. § 438.228(a).)

13) The Contractor shall ensure that individuals making decisions on the grievances and appeals of adverse benefit determinations, have the appropriate clinical expertise, as determined by the Department , in treating the beneficiary's condition or disease, if the decision involves an appeal based on a denial of medical necessity, a grievance regarding denial of a request for an expedited appeal, or if the grievance or appeal involves clinical issues.(42 C.F.R. § 438.406(b)(2)(ii)(A)-(C); 42 C.F.R. § 438.228(a).)

14) The Contractor shall provide the beneficiary a reasonable opportunity, in person and in writing, to present evidence and testimony and make legal and factual arguments. The Contractor must inform the beneficiary of the limited time available for this sufficiently in advance of the resolution timeframe for appeals specified in §438.408(b) and (c) in the case of expedited resolution. (42 C.F.R. § 438.406(b)(4).)

15) The Contractor shall ensure that decision makers on grievances and appeals of adverse benefit determinations take into account all comments, documents, records, and other information submitted by the beneficiary or beneficiary's representative, without regard to whether such information was submitted or considered in the initial adverse benefit determination. (42 C.F.R. § 438.406(b)(2)(iii); 42 C.F.R. § 438.228(a).)

16) The Contractor shall provide the beneficiary and his or her representative the beneficiary's case file, including medical records, other documents and records, and any new or additional evidence considered, relied upon, or generated by the Contractor in

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

connection with the appeal of the adverse benefit determination. (42 C.F.R. § 438.406(b)(5).)

17) The Contractor shall provide the beneficiary and his or her representative the beneficiary's case file free of charge and sufficiently in advance of the resolution timeframe for standard and expedited appeal resolutions, (42 C.F.R. § 438.408(b)-(c).) For standard resolution of an appeal and notice to the affected parties, the Contractor must comply with the Department established timeframe of 30 calendar days from the day the Contractor receives the appeal. For expedited resolution of an appeal and notice to affected parties, the Contractor must comply with the Department established timeframe of 72 hours after the Contractor receives the appeal. (42 C.F.R. § 438.406(b)(5).)

18) The Contractor shall treat oral inquiries seeking to appeal an adverse benefit determination as appeals (to establish the earliest possible filing date for the appeal) and must confirm these oral inquiries in writing, unless the beneficiary or the provider requests expedited resolution. (42 C.F.R. § 438.406(b)(3).)

19) The Contractor's beneficiary problem resolution process shall not replace or conflict with the duties of county patient's rights advocates. (Welf. & Inst. Code § 5520.)

2. Handling of Grievances and Appeals

The Contractor shall adhere to the following record keeping, monitoring, and review requirements:

A. Maintain a grievance and appeal log and record grievances, appeals, and expedited appeals in the log within one working day of the date of receipt of the grievance, appeal, or expedited appeal. (42 C.F.R. § 438.416(a); Cal. Code Regs., tit. 9, § 1850.205(d)(1).) Each record shall include, but not be limited to: a general description of the reason for the appeal or grievance the date received, the date of each review or review meeting, resolution information for each level of the appeal or grievance, if applicable, and the date of resolution at each level, if applicable, and the

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

name of the covered person whom the appeal or grievance was filed. (42 C.F.R. § 438.416(b)(1)-(6).)

B. Record in the grievance and appeal log or another central location determined by the Contractor, the final dispositions of grievances, appeals, and expedited appeals, including the date the decision is sent to the beneficiary. If there has not been final disposition of the grievance, appeal, or expedited appeal, the reason(s) shall be included in the log. (Cal. Code Regs., tit. 9, § 1850.205(d)(2).)

C. Provide a staff person or other individual with responsibility to provide information requested by the beneficiary or the beneficiary's representative regarding the status of the beneficiary's grievance, appeal, or expedited appeal. (Cal. Code Regs., tit. 9, § 1850.205(d)(3).)

D. Identify in its grievance, appeal, and expedited appeal documentation, the roles and responsibilities of the Contractor, the provider, and the beneficiary. (Cal. Code Regs., tit. 9, § 1850.205(d)(5).)

E. Provide notice, in writing, to any provider identified by the beneficiary or involved in the grievance, appeal, or expedited appeal of the final disposition of the beneficiary's grievance, appeal, or expedited appeal. (Cal. Code Regs., tit. 9, § 1850.205(d)(6).)

F. Maintain records in the grievance and appeal log accurately and in a manner accessible to the Department and available upon request to CMS. (42 C.F.R. § 438.416(c).)

3. Grievance Process

The Contractor's grievance process shall, at a minimum:

A. Allow beneficiaries to file a grievance either orally, or in writing at any time with the Contractor; (42 C.F.R. § 438.402(c)(2)(i) and (c)(3)(i).)

B. Resolve each grievance as expeditiously as the beneficiary's health condition requires not to exceed 90 calendar days from the day the Contractor receives the grievance. (42 C.F.R. § 438.408(a)-(b)(1).) The Contractor may extend the timeframe for processing a grievance by up to

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

14 calendar days if the beneficiary requests an extension, or if the Contractor determines that there is a need for additional information and that the delay is in the beneficiary's interest. (42 C.F.R. § 438.408(c)(1)(i)-(ii).) If the Contractor extends the timeframe, the Contractor shall, for any extension not requested by the beneficiary, make reasonable efforts to give the beneficiary prompt oral notice of the delay and give the beneficiary written notice of the extension and the reasons for the extension within 2 calendar days of the decision to extend the timeframe. Contractor's written notice of extension shall inform the beneficiary of the right to file a grievance if he or she disagrees with the Contractor's decision (42 C.F.R. § 438.408(c)(2)(i)-(ii).) The written notice of the extension is not a Notice of Adverse Benefit Determination. (Cal. Code Regs., tit. 9, § 1810.230.5.)

C. Provide written notification to the beneficiary or the appropriate representative of the resolution of a grievance and documentation of the notification or efforts to notify the beneficiary, if he or she could not be contacted. (Cal. Code Regs.,tit. 9, § 1850.206(c).)

D. Notify the beneficiary of the resolution of a grievance in a format and language that meets applicable notification standards. (42 C.F.R. § 438.408(d)(1); 42 C.F.R. § 438.10.)

4. Appeals Process

A. The Contractor's appeal process shall, at a minimum:

1) Allow a beneficiary, or a provider or authorized representative acting on the beneficiary's behalf, to file an appeal orally or in writing. (42 C.F.R. § 438.402(c)(3)(ii).) The beneficiary may file an appeal within 60 calendar days from the date on the adverse benefit determination notice (42 C.F.R. § 438.402(c)(2)(ii).);

2) Require a beneficiary who makes an oral appeal that is not an expedited appeal, to subsequently submit a written, signed appeal. (42 C.F.R. § 438.402(c)(3)(ii).) The Contractor shall ensure that oral inquiries seeking to appeal an adverse benefit determination are treated as appeals, and confirmed in writing unless the beneficiary or the provider requests expedited resolution. The date

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

the Contractor receives the oral appeal shall be considered the filing date for the purpose of applying the appeal timeframes (42 C.F.R. § 438.406(b)(3).);

3) Resolve each appeal and provide notice, as expeditiously as the beneficiary's health condition requires, within 30 calendar days from the day the Contractor receives the appeal. (42 C.F.R. § 438.408(a); 42 C.F.R. § 438.408(b)(2).) The Contractor may extend the timeframe for processing an appeal by up to 14 calendar days, if the beneficiary requests an extension or the Contractor determines that there is a need for additional information and that the delay is in the beneficiary's interest. (42 CFR 438.408(c)(1); 42 CFR 438.408(b)(2).) If the Contractor extends the timeframes, the Contractor shall, for any extension not requested by the beneficiary, make reasonable efforts to give the beneficiary prompt oral notice of the delay and notify the beneficiary of the extension and the reasons for the extension in writing within 2 calendar days of the decision to extend the timeframe. Contractor's written notice of extension shall inform the beneficiary of the right to file a grievance if he or she disagrees with the Contractor's decision. Contractor shall resolve the appeal as expeditiously as the beneficiary's health condition requires and no later than the date the extension expires (42 C.F.R. § 438.408(c)(2)(i)-(iii).) The written notice of the extension is not a Notice of Adverse Benefit Determination. (Cal. Code Regs., tit. 9, §1810.230.5.);

4) Allow the beneficiary to have a reasonable opportunity to present evidence and testimony and make arguments of fact or law, in person and in writing (42 C.F.R. § 438.406(b)(4).);

5) Provide the beneficiary and his or her representative the beneficiary's case file, including medical records, and any other documents and records, and any new or additional evidence considered, relied upon, or generated by the Contractor in connection with the appeal of the adverse benefit determination , provided that there is no disclosure of the protected health information of any individual other than the beneficiary (42 C.F.R. § 438.406(b)(5).); and

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

6) Provide the beneficiary and his or her representative the beneficiary's case file free of charge and sufficiently in advance of the resolution timeframe for standard appeal resolutions. For standard resolution of an appeal and notice to the affected parties, the Contractor must comply with the Department established timeframe of 30 calendar days from the day the Contractor receives the appeal. For expedited resolution of an appeal and notice to affected parties, the Contractor must comply with the Department established timeframe of 72 hours after the Contractor receives the appeal. (42 C.F.R. § 438.406(b)(5).)

7) Allow the beneficiary, his or her representative, or the legal representative of a deceased beneficiary's estate, to be included as parties to the appeal. (42 CFR 438.406(b)(6).)

B. The Contractor shall notify the beneficiary, and/or his or her representative, of the resolution of the appeal in writing in a format and language that, at a minimum, meets applicable notification standards. (42 CFR 438.408(d)(2)(i); 42 C.F.R. § 438.408(e); 42 C.F.R. 438.10.) The notice shall contain the following:

1) The results of the appeal resolution process (42 C.F.R. § 438.408(e)(1).);

2) The date that the appeal decision was made (42 C.F.R. § 438.408(e)(1).);

3) If the appeal is not resolved wholly in favor of the beneficiary, the notice shall also contain:

a) Information regarding the beneficiary's right to a fair hearing and the procedure for requesting a fair hearing, if the beneficiary has not already requested a fair hearing on the issue involved in the appeal; (42 C.F.R. § 438.408(e)(2)(i).) and

b) Information on the beneficiary's right to continue to receive benefits while the fair hearing is pending and how to request the continuation of benefits; (42 C.F.R. § 438.408(e)(2)(ii).)

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

c) Inform the beneficiary that he or she may be liable for the cost of any continued benefits if the Contractor's adverse benefit determination is upheld in the hearing. (42 C.F.R. § 438.408(e)(2)(iii).)

5. Expedited Appeal Process

A. "Expedited Appeal" is an appeal used when the mental health plan determines (for a request from the beneficiary) or the provider indicates (in making the request on the beneficiary's behalf or supporting the beneficiary's request) that taking the time for a standard resolution could seriously jeopardize the beneficiary's life, physical or mental health, or ability to attain, maintain, or regain maximum function. (42 C.F.R. 438.410.)

B. The Contractor's expedited appeal process shall, at a minimum:

1) Be used when the Contractor determines or the beneficiary and/or the beneficiary's provider certifies that taking the time for a standard appeal resolution could seriously jeopardize the beneficiary's life, physical or mental health or ability to attain, maintain, or regain maximum function. (42 C.F.R. 438.410(a).)

2) Allow the beneficiary to file the request for an expedited appeal orally without requiring the beneficiary to submit a subsequent written, signed appeal. (42 C.F.R. § 438.402(c)(3)(ii).)

3) Ensure that punitive action is not taken against a provider who requests an expedited resolution or supports a beneficiary's expedited appeal. (42 C.F.R. § 438.410(b).)

4) Inform beneficiaries of the limited time available to present evidence and testimony, in person and in writing, and make legal and factual arguments for an expedited appeal. The Contractor must inform beneficiaries of this sufficiently in advance of the resolution timeframe for the expedited appeal. (42 CFR 438.406(b)(4); 42 CFR 438.408(b)-(c).)

5) Resolve an expedited appeal and notify the affected parties in writing, as expeditiously as the beneficiary's health condition

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

requires and no later than 72 hours after the Contractor receives the appeal. (42 C.F.R. § 438.408(b)(3).) The Contractor may extend this timeframe by up to 14 calendar days if the beneficiary requests an extension, or the Contractor determines that there is need for additional information and that the delay is in the beneficiary's interest. (42 C.F.R. § 438.408(c)(1)(i)-(ii).) If the Contractor extends the timeline for processing an expedited appeal not at the request of the beneficiary, the Contractor shall make reasonable efforts to give the beneficiary prompt oral notice of the delay, and notify the beneficiary of the extension and the reasons for the extension, in writing, within 2 calendar days of the determination to extend the timeline. The Contractor shall resolve the appeal as expeditiously as the beneficiary's health condition requires and no later than the date the extension expires. (42 C.F.R. § 438.408(c)(2)(i) - (iii); 42 C.F.R. §438.408(b)(3).) The written notice of the extension is not a Notice of Adverse Benefit Determination. (Cal. Code Regs., tit. 9, § 1810.230.5.)

6) Provide a beneficiary with a written notice of the expedited appeal disposition and make reasonable efforts to provide oral notice to the beneficiary and/or his or her representative. The written notice shall meet the requirements of Section 1850.207(h) of Title 9 of the California Code of Regulations. (42 C.F.R. § 438.408(d)(2); Cal. Code Regs., tit. 9, § 1850.207(h).)

7) If the Contractor denies a request for an expedited appeal resolution, the Contractor shall:

   a) Transfer the expedited appeal request to the timeframe for standard resolution of no longer than 30 calendar days from the day the Contractor receives the appeal. (42 C.F.R. § 438.410(c)(1).)

   b) Make reasonable efforts to give the beneficiary and his or her representative prompt oral notice of the denial of the request for an expedited appeal. Provide written notice of the decision and reason for the decision within two calendar days of the date of the denial, and inform the beneficiary of the right to file a grievance if he or she disagrees with the

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

decision. (42 C.F.R. § 438.410(c)(2); 42 C.F.R. § 438.408(c)(2).) The written notice of the denial of the request for an expedited appeal is not a Notice of Adverse Benefit Determination. (Cal. Code Regs., tit. 9, § 1810.230.5.)

6. Contractor obligations related to State Fair Hearing

State "Fair Hearing" means the State hearing provided to beneficiaries pursuant to sections 50951 and 50953 of Title 22 of the California Code of Regulations section and section 1810.216.6 of Title 9 of the California Code of Regulations 1810.216.6.:

A. If a beneficiary requests a State Fair Hearing, the Department shall grant the request. (42 C.F.R. § 431.220(a)(5).) The right to a State Fair Hearing, how to obtain a hearing, and representation rules at a hearing must be explained to the beneficiary and provider by Contractor in its notice of decision or Notice of Adverse Benefit Determination. (42 C.F.R. § 431.206(b); 42 C.F.R. § 431.228(b).) Beneficiaries and providers shall also be informed of the following:

1) A beneficiary may request a State Fair Hearing only after receiving notice that the Contractor is upholding the adverse benefit determination. (42 C.F.R. § 438.408(f)(1).)

2) If the Contractor fails to adhere to notice and timing requirements under § 438.408, the beneficiary is deemed to have exhausted the Contractor's appeals process, and the beneficiary may initiate a state fair hearing. (42 CFR 438.408(f)(1)(i); 42 CFR 438.402(c)(1)(i)(A).)

3) The provider may request a State Fair Hearing only if the Department permits the provider to act as the beneficiary's authorized representative. (42 C.F.R. § 438.402(c)(1)(ii).)

7. Expedited Fair Hearing

"Expedited Fair Hearing" means a fair hearing, used when the Contractor determines, or the beneficiary or the beneficiary's provider certifies that following the 90 day timeframe for a fair hearing as established in 42 C.F.R. §

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

431.244(f)(1) would seriously jeopardize the beneficiary's life, health, or ability to attain, maintain, or regain maximum function. (42 C.F.R. § 431.244(f)(1); 42 C.F.R. § 438.410(a); Cal. Code Regs., tit. 9, § 1810.216.4.)

8. Continuation of Services

A. A beneficiary receiving specialty mental health services shall have a right to file for continuation of specialty mental health services pending the outcome of a fair hearing. (Cal. Code Regs., tit. 22., § 51014.2; Cal. Code Regs., tit. 9, § 1850.215.)

B. The Contractor shall continue the beneficiary's benefits while an appeal is in process if all of the following occur:

1) The beneficiary files the request for an appeal within 60 calendar days following the date on the adverse benefit determination notice; (42 C.F.R. § 438.420(b)(1).)

2) The appeal involves the termination, suspension, or reduction of a previously authorized service; (42 C.F.R. § 438.420(b)(2).)

3) The beneficiary's services were ordered by an authorized provider; (42 C.F.R. § 438.420(b)(3).)

4) The period covered by the original authorization has not expired; and, (42 C.F.R. § 438.420(b)(4).)

5) The request for continuation of benefits is filed on or before the later of the following: (42 C.F.R. § 438.420 (b)(5).)

a. Within 10 calendar days of the Contractor sending the notice of adverse benefit determination; (42 C.F.R. § 438.420(a).) or

b. The intended effective date of the adverse benefit determination. (42 C.F.R. § 438.420(a).)

C. If, at the beneficiary's request, the Contractor continues the beneficiary's benefits while the appeal or state fair hearing is pending, the benefits must

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

be continued until the beneficiary withdraws the appeal or request for state fair hearing, the beneficiary does not request a state fair hearing and continuation of benefits within 10 calendar days from the date the Contractor sends the notice of an adverse appeal resolution, or a state fair hearing decision adverse to the beneficiary is issued. (42 C.F.R. § 438.420(c)(1)-(3); 42 C.F.R. § 438.408(d)(2).)

D. The Contractor may recover the cost of continued services furnished to the beneficiary while the appeal or state fair hearing was pending if the final resolution of the appeal or state fair hearing upholds the Contractor's adverse benefit determination. (42 C.F.R. § 438.420(d); 42 C.F.R. § 431.230(b).)

E. The Contractor shall authorize or provide the disputed services promptly, and as expeditiously as the beneficiary's health condition requires, but no later than 72 hours from the date the Contractor receives notice reversing the determination if the services were not furnished while the appeal was pending and if the Contractor or state fair hearing officer reverses a decision to deny, limit, or delay services. (42 C.F.R. § 438.424(a).)

F. If the decision of an appeal reverses a decision to deny the authorization of services, and the beneficiary received the disputed services while the appeal was pending, the Contractor shall cover the cost of such services. (42 C.F.R. § 438.424(b).)

G. The Contractor shall notify the requesting provider and give the beneficiary written notice of any decision to deny a service authorization request, or to authorize a service in an amount, duration, or scope that is less than requested. (42 C.F.R. § 438.210(c); 42 C.F.R. § 438.404.)

9. Provision of Notice of Adverse Benefit Determination

A. The Contractor shall provide a beneficiary with a Notice of Adverse Benefit Determination (NOABD) under the following circumstances:

1) The denial or limited authorization of a requested service, including determinations based on the type or level of service, requirements for medical necessity, appropriateness, setting, or effectiveness of a covered benefit. (42 C.F.R. § 438.400(b)(1).)

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

2) The reduction, suspension, or termination of a previously authorized service. (42 C.F.R. § 438.400(b)(2).)

3) The denial, in whole or in part, of payment for a service. (42 C.F.R. § 438.400(b)(3).)

4) The failure to provide services in a timely manner, as defined by the Department. (42 C.F.R. § 438.400(b)(4).)

5) The failure of the Contractor to act within the timeframes provided in §438.408(b)(1) and (2) regarding the standard resolution of grievances and appeals. (42 C.F.R. § 438.400(b)(5).)

6) The denial of a beneficiary's request to dispute a financial liability, including cost sharing, copayments, premiums, deductibles, coinsurance, and other beneficiary financial liabilities. (42 C.F.R. § 438.400(b)(7).)

B. The Contractor shall give beneficiaries timely and adequate notice of an adverse benefit determination in writing and shall meet the language and format requirements of 42 Code of Federal Regulations part 438.10. (42 C.F.R. § 438.404(a); 42 C.F.R. § 438.10.) The NOA shall contain the items specified in 42 Code of Federal Regulations part 438.404 (b) and California Code of Regulations, title 9, section 1850.212.

C. When the denial or modification involves a request from a provider for continued Contractor payment authorization of a specialty mental health service or when the Contractor reduces or terminates a previously approved Contractor payment authorization, notice shall be provided in accordance with California Code of Regulations, title 22, section 51014.1. (Cal. Code Regs., tit. 9, § 1850.210(a)(1).)

D. A NOABD is not required when a denial is a non-binding verbal description to a provider of the specialty mental health services that may be approved by the Contractor. (Cal. Code Regs., tit. 9, § 1850.210(a)(2).)

E. Except as provided in subsection F below, a NOABD is not required when the denial or modification is a denial or modification of a request for

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

Contractor payment authorization for a specialty mental health service that has already been provided to the beneficiary. (Cal. Code Regs., tit. 9, § 1850.210(a)(4).)

F. A NOABD is required when the Contractor denies or modifies a payment authorization request from a provider for a specialty mental health service that has already been provided to the beneficiary when the denial or modification is a result of post-service, prepayment determination by the Contractor that the service was not medically necessary or otherwise was not a service covered by the Contractor. (Cal. Code Regs., tit. 9, § 1850.210(b).)

G. The Contractor shall deny the Contractor payment authorization request and provide the beneficiary with a NOABD when the Contractor does not have sufficient information to approve or modify, or deny on the merits, a Contractor payment authorization request from a provider within the timeframes required by Cal. Code Regs., tit. 9, §§ 1820.220 or 1830.215. (Cal. Code Regs., tit. 9, § 1850.210(c).)

H. The Contractor shall provide the beneficiary with a NOABD if the Contractor fails to notify the affected parties of a resolution of a grievance within 90 calendar days, of an appeal decision within 30 days, or of an expedited appeal decision within 72 hours. If the timeframe for a grievance, appeal or expedited appeal decision is extended pursuant to sections 1850.206, 1850.207 or 1850.208 of Title 9 of the California Code of Regulations and the Contractor failed to notify the affected parties of its decision within the extension period, the Contractor shall provide the beneficiary with a NOABD. (42 C.F.R. § 438.408.)

I. The Contractor shall provide a beneficiary with a NOABD when the Contractor or its providers determine that the medical necessity criteria in sections 1830.205(b)(1),(b)(2),(b)(3)(C), or 1830.210(a) of Title 9 of the California Code of Regulations have not been met and that the beneficiary is not entitled to any specialty mental health services from the Contractor. The NOABD shall, at the election of the Contractor, be hand-delivered to the beneficiary on the date of the Adverse Benefit Determination or mailed to the beneficiary in accordance with Cal. Code Regs., tit. 9, § 1850.210(f)(1), and shall specify the information contained in Cal. Code Regs., tit. 9, § 1850.212(b). (Cal. Code Regs., tit. 9, § 1850.210(g).)

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

J. For the purpose of this Attachment, each reference to a Medi-Cal managed care plan in Cal. Code Regs., tit. 22, § 51014.1, shall mean the Contractor. (Cal. Code Regs., tit. 9, § 1850.210(h).)

K. For the purposes of this Attachment, "medical service", as used in Cal. Code Regs., tit. 22, § 51014.1, shall mean specialty mental health services that are subject to prior authorization by a Contractor pursuant to Cal. Code Regs., tit. 9, §§ 1820.100 and 1830.100. (Cal. Code Regs., tit. 9, § 1850.210(i).)

L. The Contractor shall retain copies of all Notices of Adverse Benefit Determination issued to beneficiaries under this Section in a centralized file accessible to the Department. The Department shall engage in random reviews (Cal. Code Regs., tit. 9, § 1850.210(j).)

M. The Contractor shall allow the State to engage in reviews of the Contractor's records pertaining to Notices of Adverse Benefit Determination so the Department may ensure that the Contractor is notifying beneficiaries in a timely manner.

10. Contents and Timing of NOABD

A. The Contractor shall include the following information in the NOABD:

1) The adverse benefit determination the Contractor has made or intends to make; (42 C.F.R. § 438.404(b)(1).)

2) The reason for the adverse benefit determination, including the right of the beneficiary to be provided upon request and free of charge, reasonable access to and copies of all documents, records, and other information relevant to the beneficiary's adverse benefit determination. Such information includes medical necessity criteria, and any processes, strategies, or evidentiary standards used in setting coverage limits; (42 C.F.R. § 438.404(b)(2).)

3) Citations to the regulations or Contractor payment authorization procedures supporting the adverse benefit determination; (Cal. Code Regs., tit. 9, § 1850.212(a)(3).)

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

4) The beneficiary's right to file, and procedures for exercising, an appeal or expedited appeal with the Contractor, including information about exhausting the Contractor's one level of appeal and the right to request a state fair hearing after receiving notice that the adverse benefit determination is upheld; (42 C.F.R. § 438.404(b)(3)-(b)(4).)

5) The circumstances under which an appeal process can be expedited and how to request it; (42 C.F.R. § 438.404(b)(5).)

6) The beneficiary's right to have benefits continue pending resolution of the appeal, how to request that benefits be continued, and the circumstances under which the beneficiary may be required to pay the costs of those services. (42 C.F.R. § 438.404(b)(6).)

7) Information about the beneficiary's right to request a fair hearing or an expedited fair hearing, including:

   a) The method by which a hearing may be obtained; (Cal. Code Regs., tit. 9, § 1850.212(a)(5)(A).)

   b) A statement that the beneficiary may be either self-represented, or represented by an authorized third party such as legal counsel, a relative, friend, or any other person; (Cal. Code Regs., tit. 9, § 1850.212(a)(5)(B).)

   c) An explanation of the circumstances under which a specialty mental health service will be continued if a fair hearing is requested; (Cal. Code Regs., tit. 9, § 1850.212(a)(5)(C).) and

   d) The time limits for requesting a fair hearing or an expedited fair hearing. (Cal. Code Regs., tit. 9, § 1850.212(a)(5)(D).)

B. The Contractor shall mail the NOABD within the following timeframes:

1) For termination, suspension, or reduction of previously authorized Medi-Cal covered services, at least 10 days before the date of

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

action. (42 C.F.R. § 438.404(c)(1); 42 C.F.R. § 431.211.) The Contractor shall mail the NOABD in as few as 5 days prior to the date of action if the Contractor has facts indicating that action should be taken because of probable fraud by the beneficiary, and the facts have been verified, if possible, through secondary sources. (42 C.F.R. § 438.404(c)(1); 42 C.F.R. §.431.214.)

2) For denial of payment, at the time of any action affecting the claim. (42 C.F.R. § 438.404(c)(2).)

3) For standard service authorizations that deny or limit services, as expeditiously as the beneficiary's condition requires not to exceed 14 calendar days following the receipt for request for services. (42 C.F.R. § 438.404(c)(3); 42 C.F.R. 438.210(d)(1).)

4) The Contractor may extend the 14 calendar day NOABD determination timeframe for standard service authorization decisions that deny or limit services up to 14 additional calendar days if the beneficiary or the provider requests the extension. (42 C.F.R. § 438.404(c)(4); 42 C.F.R. 438.210(d)(1)(i).)

5) The Contractor may extend the 14 calendar day notice of adverse benefit determination timeframe for standard service authorization decisions that deny or limit services up to 14 additional calendar days if the Contractor justifies a need to the Department, upon request, for additional information and shows how the extension is in the beneficiary's best interest. (42 C.F.R. § 438.404(c)(4); 42 C.F.R. 438.210(d)(1)(ii).)

6) If the Contractor extends the 14 calendar day notice of adverse benefit determination timeframe for standard service authorization decisions that deny or limit services, the Contractor shall do the following:

   a) Give the beneficiary written notice of the reason for the extension and inform the beneficiary of the right to file a grievance if he/she disagrees with the decision ; (42 C.F.R. § 438.404(c)(4)(i); 42 C.F.R. 438.210(d)(1)(ii).) and,

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

b) Issue and carry out its determination as expeditiously as the beneficiary's health condition requires and no later than the date of the extension. (42 C.F.R. § 438.404(c)(4)(ii); 42 C.F.R. 438.210(d)(1)(ii).)

7) The Contractor shall give notice on the date that the timeframes expire, when service authorization decisions are not reached within the applicable timeframes for either standard or expedited service authorizations. (42 C.F.R. § 438.404(c)(5).)

8) If a provider indicates, or the Contractor determines, that following the standard service authorization timeframe could seriously jeopardize the beneficiary's life or health or his or her ability to attain, maintain, or regain maximum function, the Contractor must make an expedited service authorization decision and provide notice as expeditiously as the beneficiary's health condition requires and no later than 72 hours after receipt of the request for service. (42 C.F.R. § 438.404(c)(6); 42 C.F.R. 438.210(d)(2)(i).)

9) The Contractor may extend the 72 hour expedited service authorization decision time period by up to 14 calendar days if the beneficiary requests an extension, or if the Contractor justifies to the Department, upon request, a need for additional information and how the extension is in the beneficiary's interest. (42 C.F.R. § 438.404(c)(6); 42 C.F.R. § 210(d)(2)(ii).)

10) The Contractor shall deposit the NOABD with the United States Postal Service in time for pick-up on the date that the applicable timeframe expires. (Cal. Code Regs., tit. 9, § 1850.210(f).)

C. The Adverse Benefit Determination shall be effective on the date of the NOABD and the Contractor shall mail the NOABD by the date of adverse benefit determination when any of the following occur:

1) The death of a beneficiary; (42 C.F.R. § 431.213(a).)

2) Receipt of a signed written beneficiary statement requesting service termination or giving information requiring termination or reduction of services, provided the beneficiary understands that this will be

Exhibit A – Attachment 12
BENEFICIARY PROBLEM RESOLUTION

the result of supplying that information; (42 C.F.R. § 431.213(b)(1)-(b)(2).)

3) The beneficiary's admission to an institution where he or she is ineligible for further services; (42 C.F.R. § 431.213(c).)

4) The beneficiary's whereabouts are unknown and mail directed to him or her has no forwarding address; (42 C.F.R. § 431.213(d).)

5) Notice that the beneficiary has been accepted for Medicaid services by another local jurisdiction; (42 C.F.R. § 431.213(e).)

6) A change in the beneficiary's physician's prescription for the level of medical care; (42 C.F.R. § 431.213(f).) or

7) The notice involves an adverse determination with regard to preadmission screening requirements of section 1919(e)(7) of the Act. (42 C.F.R. § 431.213(g).)

8) The transfer or discharge from a facility will occur in an expedited fashion. (42 C.F.R. § 431.213(h).)

9) Endangerment of the safety or health of individuals in the facility; improvement in the resident's health sufficient to allow a more immediate transfer or discharge; urgent medical needs that require a resident's immediate transfer or discharge; or notice that a resident has not resided in the nursing facility for 30 days (but only in Adverse Benefit Determinations based on NF transfers).

11. Annual Grievance and Appeal Report

The Contractor is required to submit to the Department a report that summarizes beneficiary grievances, appeals and expedited appeals filed from July 1 of the previous year through June 30 of that year by October 1 of each year. The report shall include the total number of grievances, appeals and expedited appeals by type, by subject areas established by the Department, and by disposition. (Cal. Code Regs., tit. 9, § 1810.375(a).)

Exhibit A – Attachment 13
PROGRAM INTEGRITY

1. General Requirements

As a condition for receiving payment under a Medi-Cal managed care program, the Contractor shall comply with the provisions of 42 C.F.R. §§ 438.604, 438.606 and 438.608, and 438.610. (42 C.F.R. § 438.600(b).)

2. Excluded Providers

A. The Contractor shall screen and periodically revalidate all network providers in accordance with the requirements of 42 Code of Federal Regulations, part 455, subparts B and E. (42 C.F.R. §438.602(b).)

B. Consistent with the requirements of 42 Code of Federal Regulations, part 455.436, the Contractor must confirm the identity and determine the exclusion status of all providers (employees and network providers) and any subcontractor, as well as any person with an ownership or control interest, or who is an agent or managing employee of the of the Mental Health Plan through routine checks of Federal and State databases. This includes the Social Security Administration's Death Master File, the National Plan and Provider Enumeration System (NPPES), the Office of Inspector General's List of Excluded Individuals/Entities (LEIE), the System for Award Management (SAM), as well as the Department's Medi Cal Suspended and Ineligible Provider List (S & I List). (42 C.F.R. §438.602(d).)

C. If the Contractor find a party that is excluded, it must promptly notify the Department (42 C.F.R. §438.608(a)(2),(4)) and the Department will take action consistent with 42 C.F.R. §438.610((d). The Contractor shall not certify or pay any excluded provider with Medi-Cal funds, and any such inappropriate payments or overpayments may be subject to recovery and/or be the basis for other sanctions by the appropriate authority.

3. Compliance Program

A. Pursuant to 42 C.F.R. § 455.1(a)(1), the Contractor must report fraud and abuse information to the Department.

B. The Contractor, or any subcontractor, to the extent that the subcontractor is delegated responsibility by the Contractor for coverage of services and

Exhibit A – Attachment 13
PROGRAM INTEGRITY

payment of claims under this Contract, shall implement and maintain a compliance program designed to detect and prevent fraud, waste and abuse that must include:

1) Written policies, procedures, and standards of conduct that articulate the organization's commitment to comply with all applicable requirements and standards under the contract, and all applicable Federal and state requirements.

2) A Compliance Officer (CO) who is responsible for developing and implementing policies, procedures, and practices designed to ensure compliance with the requirements of the contract and who reports directly to the CEO and the Board of Directors (BoD).

3) A Regulatory Compliance Committee (RCC) on the BoD and at the senior management level charged with overseeing the organization's compliance program and its compliance with the requirements under the contract.

4) A system for training and education for the CO, the organization's senior management, and the organization's employees for the federal and state standards and requirements under the contract.

5) Effective lines of communication between the CO and the organization's employees.

6) Enforcement of standards through well-publicized disciplinary guidelines.

7) The establishment and implementation of procedures and a system with dedicated staff for routine internal monitoring and auditing of compliance risks, prompt response to compliance issues as they are raised, investigation of potential compliance problems as identified in the course of self-evaluation and audits, correction of such problems promptly and thoroughly (or coordination of suspected criminal acts with law enforcement agencies) to reduce the potential for recurrence, and ongoing compliance with the requirements under the contract. (42 C.F.R. §438.608(a), (a)(1).)

Exhibit A – Attachment 13
PROGRAM INTEGRITY

4. Fraud Reporting Requirements

A. The Contractor, or any subcontractor, to the extent that the subcontractor is delegated responsibility by the Contractor for coverage of services and payment of claims under this Contract, shall implement and maintain arrangements or procedures designed to detect and prevent fraud, waste and abuse that include prompt reporting to the Department about the following:

1) Any potential fraud, waste, or abuse. (42 C.F.R. §438.608(a), (a)(7).)

2) All overpayments identified or recovered, specifying the overpayments due to potential fraud. (42 C.F.R. §438.608(a), (a)(2).)

3) Information about changes in a beneficiary's circumstances that may affect the beneficiary's eligibility including changes in the beneficiary's residence or the death of the beneficiary. (42 C.F.R. §438.608(a), (a)(3).)

4) Information about a change in a network provider's circumstances that may affect the network provider's eligibility to participate in the managed care program, including the termination of the provider agreement with the Contractor. (42 C.F.R. §438.608(a), (a)(4).)

B. If the Contractor identifies an issue or receives notification of a complaint concerning an incident of potential fraud, waste or abuse, in addition to notifying the Department, the Contractor shall conduct an internal investigation to determine the validity of the issue/complaint, and develop and implement corrective action, if needed.

C. The Contractor shall implement and maintain written policies for all employees of the Mental Health Plan, and of any contractor or agent, that provide detailed information about the False Claims Act and other Federal and state laws, including information about rights of employees to be protected as whistleblowers. (42 C.F.R. §438.608(a), (a)(6).)

Exhibit A – Attachment 13
PROGRAM INTEGRITY

D. The Contractor shall implement and maintain arrangements or procedures that include provision for the Contractor's suspension of payments to a network provider for which there is a credible allegation of fraud. (42 C.F.R. §438.608(a), (a)(8).)

5. Service Verification

Pursuant to 42 C.F.R. § 438.608(a)(5), the Contractor, and/or any subcontractor, to the extent that the subcontractor is delegated responsibility by the Contractor for coverage of services and payment of claims under this Contract, shall implement and maintain arrangements or procedures designed to detect and prevent fraud, waste and abuse that include provisions to verify, by sampling or other methods, whether services that have been represented to have been delivered by network providers were received by beneficiaries and the application of such verification processes on a regular basis. (42 C.F.R. §438.608(a), (a)(5).)

6. Disclosures

A. Disclosure of 5% or More Ownership Interest:

1) Pursuant to 42 C.F.R. § 455.104, Medicaid managed care entities must disclose certain information related to persons who have an ownership or control interest in the managed care entity, as defined in 42 C.F.R. § 455.101. The parties hereby acknowledge that because the Contractor is a political subdivision of the State of California, there are no persons who meet such definition and therefore there is no information to disclose.

a) In the event that, in the future, any person obtains an interest of 5% or more of any mortgage, deed of trust, note or other obligation secured by Contractor, and that interest equals at least 5% of Contractor's property or assets, then the Contractor will make the disclosures set forth in i and subsection 2(a).

i. The Contractor will disclose the name, address, date of birth, and Social Security Number of any managing employee, as that term is defined in 42 C.F.R. §

Exhibit A – Attachment 13
PROGRAM INTEGRITY

455.101. For purposes of this disclosure, Contractor may use the business address for any member of its Board of Supervisors.

ii. The Contractor shall provide any such disclosure upon execution of this contract, upon its extension or renewal, and within 35 days after any change in Contractor ownership or upon request of the Department.

2) The Contractor shall ensure that its subcontractors and network providers submit the disclosures below to the Contractor regarding the network providers' (disclosing entities') ownership and control. The Contractor's network providers must be required to submit updated disclosures to the Contractor upon submitting the provider application, before entering into or renewing the network providers' contracts, within 35 days after any change in the subcontractor/network provider's ownership, annually and upon request during the re-validation of enrollment process under 42 Code of Federal Regulations part 455.104.

a) Disclosures to be Provided:

i. The name and address of any person (individual or corporation) with an ownership or control interest in the network provider. The address for corporate entities shall include, as applicable, a primary business address, every business location, and a P.O. Box address;

ii. Date of birth and Social Security Number (in the case of an individual);

iii. Other tax identification number (in the case of a corporation with an ownership or control interest in the managed care entity or in any subcontractor in which the managed care entity has a 5 percent or more interest);

iv. Whether the person (individual or corporation) with an ownership or control interest in the Contractor's network provider is related to another person with

Exhibit A – Attachment 13
PROGRAM INTEGRITY

ownership or control interest in the same or any other network provider of the Contractor as a spouse, parent, child, or sibling; or whether the person (individual or corporation) with an ownership or control interest in any subcontractor in which the managed care entity has a 5 percent or more interest is related to another person with ownership or control interest in the managed care entity as a spouse, parent, child, or sibling;

v. The name of any other disclosing entity in which the Contractor or subcontracting network provider has an ownership or control interest; and

vi. The name, address, date of birth, and Social Security Number of any managing employee of the managed care entity.

3) For each provider in Contractor's provider network, Contractor shall provide the Department with all disclosures before entering into a network provider contract with the provider and annually thereafter and upon request from the Department during the re-validation of enrollment process under 42 Code of Federal Regulations part 455.104.

B. Disclosures Related to Business Transactions – Contractor must submit disclosures and updated disclosures to the Department or HHS including information regarding certain business transactions within 35 days, upon request.

1) The following information must be disclosed:

a) The ownership of any subcontractor with whom the Contractor has had business transactions totaling more than $25,000 during the 12-month period ending on the date of the request; and

b) Any significant business transactions between the Contractor and any wholly owned supplier, or between the Contractor and any subcontractor, during the 5-year period ending on the date of the request.

Exhibit A – Attachment 13
PROGRAM INTEGRITY

c) Contractor must obligate Network Providers to submit the same disclosures regarding network providers as noted under subsection 1(a) and (b) within 35 days upon request.

C. Disclosures Related to Persons Convicted of Crimes

1) Contractor shall submit the following disclosures to the Department regarding the Contractor's management:

a) The identity of any person who is a managing employee of the Contractor who has been convicted of a crime related to federal health care programs. (42 C.F.R. § 455.106(a)(1), (2).)

b) The identity of any person who is an agent of the Contractor who has been convicted of a crime related to federal health care programs. (42 C.F.R. § 455.106(a)(1), (2).) For this purpose, the word "agent" has the meaning described in 42 Code of Federal Regulations part 455.101.

2) The Contractor shall supply the disclosures before entering into the contract and at any time upon the Department's request.

3) Network providers should submit the same disclosures to the Contractor regarding the network providers' owners, persons with controlling interest, agents, and managing employees' criminal convictions. Network providers shall supply the disclosures before entering into the contract and at any time upon the Department's request.

Exhibit A – Attachment 14
REPORTING REQUIREMENTS

1. Data Submission/ Certification Requirements

A. The Contractor shall submit any data, documentation, or information relating to the performance of the entity's obligations as required by the State or the United States Secretary of Health and Human Services. (42 C.F.R. § 438.604(b).) The individual who submits this data to the state shall concurrently provide a certification, which attests, based on best information, knowledge and belief that the data, documentation and information is accurate, complete and truthful. (42 C.F.R. § 438.606(b) and (c).)The data, documentation, or information submitted to the state by the Contractor shall be certified by one of the following:

1) The Contractor's Chief Executive Officer (CEO).

2) The Contractor's Chief Financial Officer (CFO).

3) An individual who reports directly to the CEO or CFO with delegated authority to sign for the CEO or CFO so that the CEO or CFO is ultimately responsible for the certification. (42 C.F. R. § 438.606(a).)

2. Encounter Data

The Contractor shall submit encounter data to the Department at a frequency and level specified by the Department and CMS. (42 C.F.R. § 438.242(c)(2).) The Contractor shall ensure collection and maintenance of sufficient beneficiary encounter data to identify the provider who delivers service(s) to the beneficiary. (42 C.F.R. § 438.242(c)(1).) The Contractor shall submit all beneficiary encounter data that the Department is required to report to CMS under § 438.818. (42 C.F.R. § 438.242(c)(3).) The Contractor shall submit encounter data to the state in standardized Accredited Standards Committee (ASC) X12N 837 and National Council for Prescription Drug Programs (NCPDP) formats, and the ASC X12N 835 format as appropriate. (42 C.F.R. § 438.242(c)(4).)

3. Insolvency

A. The Contractor shall submit data to demonstrate it has made adequate provision against the risk of insolvency to ensure that beneficiaries will not

Exhibit A – Attachment 14
REPORTING REQUIREMENTS

be liable for the Contractor's debt if the Contractor becomes insolvent. (42 C.F.R. § 438.604(a)(4); 42 C.F.R . § 438.116.)

B. The Contractor shall meet the State's solvency standards for private health maintenance organizations or be licensed by the State as a risk-bearing entity, unless one of the following exceptions apply (42 C.F.R. § 438.116 (b).):

1) The Contractor does not provide both inpatient hospital services and physician services.
2) The Contractor is a public entity.
3) The Contractor is (or is controlled by) one of more federally qualified health centers and meets the solvency standards established by the State for those centers.
4) The Contractor has its solvency guaranteed by the State.

4. Network Adequacy

The Contractor shall submit, in a manner and format determined by the Department, documentation to demonstrate compliance with the Department's requirements for availability and accessibility of services, including the adequacy of the provider network. (42 C.F.R. § 438.604(a)(5).)

5. Information on Ownership and Control

The Contractor shall submit for state review information on its and its subcontractors' ownership and control described in 42 C.F.R. §455.104 and Attachment 13 of this Contract. (42 C.F.R § 438.604(a)(6).)

6. Annual Report of Overpayment Recoveries

The Contractor shall submit an annual report of overpayment recoveries in a manner and format determined by the Department. (42 C.F.R § 438.604(a)(7).)

7. Performance Data

A. In an effort to improve the performance of the State's managed care program, in accordance with 42 Code of Federal Regulations part

Exhibit A – Attachment 14
REPORTING REQUIREMENTS

438.66(c), the Contractor will submit the following to the Department (42 C.F.R. §438.604(b).):

1) Enrollment and disenrollment data;

2) Member grievance and appeal logs;

3) Provider complaint and appeal logs;

4) The results of any beneficiary satisfaction survey;

5) The results of any provider satisfaction survey;

6) Performance on required quality measures;

7) Medical management committee reports and minutes;

8) The Contractor's annual quality improvement plan;

9) Audited financial and encounter data; and

10) Customer service performance data.

Exhibit B
BUDGET DETAIL AND PAYMENT PROVISIONS

1. Payment Provisions

This program may be funded using one or more of the following funding sources: funds distributed to the counties from the Mental Health Subaccount, the Mental Health Equity Subaccount, and the Vehicle License Collection Account of the Local Revenue Fund, funds from the Mental Health Account and the Behavioral Health Subaccount of the Local Revenue Fund 2011, funds from the Mental Health Services Fund, and any other funds from which the Controller makes distributions to the counties in compliance with applicable statute and regulations including Welf. & Inst. Code §§ 5891, 5892 and 14705(a)(2). These funding sources may be used by the Contractor to pay for services and then certify as public expenditures in order to be reimbursed federal funds.

2. Budget Contingency Clause

This provision is a supplement to provision number nine (Federal Contract Funds) in Exhibit D(F) which is attached hereto as part of this Contract.

A. Federal Budget
If federal funding for FFP reimbursement in relation to this contract is eliminated or substantially reduced by Congress, the Department and the Contractor each shall have the option either to cancel this contract or to propose a contract amendment to address changes to the program required as a result of the elimination or reduction of federal funding.

B. Delayed Federal Funding

Contractor and Department agree to consult with each other on interim measures for program operation that may be required to maintain adequate services to beneficiaries in the event that there is likely to be a delay in the availability of federal funding.

3. Federal Financial Participation

Nothing in this contract shall limit the Contractor's ability to submit claims for appropriate FFP reimbursement based on actual, total fund expenditures for any covered services or quality assurance, utilization review, Medi-Cal Administrative Activities and/or administrative costs. In accordance the Welf. & Inst. Code § 14705(c), the Contractor shall ensure compliance with all requirements necessary for Medi-Cal reimbursement for these services and activities. Claims for FFP reimbursement shall be submitted by the Contractor to the Department for adjudication throughout the fiscal year. Pursuant to the

Exhibit B
BUDGET DETAIL AND PAYMENT PROVISIONS

Welf. & Inst. Code § 14705(d), the Contractor shall certify to the state that it has incurred public expenditures prior to requesting the reimbursement of federal funds.

4. Audits and Recovery of Overpayments

A. Pursuant to Welf. & Inst. Code § 14707, in the case of federal audit exceptions, the Department will follow federal audit appeal processes unless the Department, in consultation with the California Mental Health Director's Association, determines that those appeals are not cost beneficial.

1) Whenever there is a final federal audit exception against the State resulting from a claim for federal funds for an expenditure by individual counties that is not federally allowable, the department may offset federal reimbursement and request the Controller's office to offset the distribution of funds to the Contractor from the Mental Health Subaccount, the Mental Health Equity Subaccount and the Vehicle License Collection Account of the Local Revenue Fund; funds from the Mental Health Account and the Behavioral Health Subaccount of the Local Revenue Fund 2011; and any other mental health realignment funds from which the Controller makes distributions to the counties by the amount of the exception. The Department shall provide evidence to the Controller that the county had been notified of the amount of the audit exception no less than 30 days before the offset is to occur.

2) The Department will involve the Contractor in developing responses to any draft federal audit reports that directly impact the county.

B. Pursuant to Welf. & Inst. Code § 14718(b)(2), the Department may offset the amount of any federal disallowance, audit exception, or overpayment against subsequent claims from the Contractor.

1) The Department may offset the amount of any state disallowance, audit exception, or overpayment for fiscal years through and including 2010-11 against subsequent claims from the Contractor.

2) Offsets may be done at any time, after the department has invoiced or otherwise notified the Contractor about the audit exception, disallowance, or overpayment. The Department shall determine the amount that may be withheld from each payment to the mental health plan.

Exhibit B
BUDGET DETAIL AND PAYMENT PROVISIONS

3) The maximum withheld amount shall be 25 percent of each payment as long as the Department is able to comply with the federal requirements for repayment of FFP pursuant 42 United States Code (U.S.C.) §1396b(d)(2)). The Department may increase the maximum amount when necessary for compliance with federal laws and regulations.

C. Pursuant to the Welf. & Inst. Code § 14170, cost reports submitted to the Department are subject to audit in the manner and form prescribed by the Department. The year-end cost report shall include both Contractor's costs and the costs of its subcontractors, if any. Contractor and its subcontractors shall be subject to audits and/or reviews, including client record reviews, by the Department. In accordance with the Welf. & Inst. Code § 14170, any audit of Contractor's cost report shall occur within three years of the date of receipt by the Department of the final cost report with signed certification by the Contractor's Mental Health Director and one of the following: (1) the Contractor's Chief Financial Officer (or equivalent), (2) an individual who has delegated authority to sign for, and reports directly to the Contractor's Chief Financial Officer, or (3) the county auditor controller, or equivalent. Both signatures are required before the cost report shall be considered final. For purposes of this section, the cost report shall be considered audited once the Department has informed the Contractor of its intent to disallow costs on the cost report, or once the Department has informed the Contractor of its intent to close the audit without disallowances.

D. If the adjustments result in the Department owing FFP to the Contractor, the Department shall submit a claim to the federal government for the related FFP within 30 days contingent upon sufficient budget authority.

5. Claims Adjudication Process

A. In accordance with the Welf. & Inst. Code §14705(c), claims for federal funds in reimbursement for services shall comply with eligibility and service requirements under applicable federal and state law.

B. The Contractor shall certify each claim submitted to the Department in accordance with Cal. Code Regs., tit. 9, § 1840.112 and 42 C.F.R. § 433.51, at the time the claims are submitted to the Department. The Contractor's Chief Financial Officer or his or her equivalent, or an individual with authority delegated by the county auditor-controller, shall sign the certification, declaring, under penalty of perjury, that the Contractor has incurred an expenditure to cover the services included in the claims to satisfy the requirements for FFP. The Contractor's Mental Health Director or an individual with authority delegated by the Mental Health Director

Exhibit B
BUDGET DETAIL AND PAYMENT PROVISIONS

shall sign the certification, declaring, under penalty of perjury that, to the best of his or her knowledge and belief, the claim is in all respects true, correct, and in accordance with the law and meets the requirements of Cal. Code Regs., tit. 9, § 1840.112(b). The Contractor shall have mechanisms that support the Mental Health Director's certification, including the certification that the services for which claims were submitted were actually provided to the beneficiary. If the Department requires additional information from the Contractor that will be used to establish Department payments to the Contractor, the Contractor shall certify that the additional information provided is in accordance with 42 C.F.R. § 438.604.

C. Claims not meeting federal and/or state requirements shall be returned to Contractor as not approved for payment, along with a reason for denial. Claims meeting all Health Insurance Portability and Accountability Act (HIPAA) transaction requirements and any other applicable federal or state privacy laws or regulations and certified by the Contractor in accordance with Cal. Code Regs., tit. 9, §1840.112, shall be processed for adjudication.

D. Good cause justification for late claim submission is governed by applicable federal and state laws and regulations and is subject to approval by the Department.

E. In the event that the Department or the Contractor determines that changes requiring a change in the Contractor's or Department's obligation must be made relating to either the Department's or the Contractor's claims submission and adjudication systems due to federal or state law changes or business requirements, both the Department and the Contractor agree to provide notice to the other party as soon as practicable prior to implementation. This notice shall include information and comments regarding the anticipated requirements and impacts of the projected changes. The Department and the Contractor agree to meet and discuss the design, development, and costs of the anticipated changes prior to implementation.

F. The Contractor shall comply with Cal. Code Regs., tit. 9, § 1840.304, when submitting claims for FFP for services billed by individual or group providers. The Contractor shall submit service codes from the Health Care Procedure Coding System (HCPCS) published in the most current Mental Health Medi-Cal billing manual.

6. **Payment Data Certification**

Contractor shall certify the data it provides to the Department to be used in determining payment of FFP to the Contractor, in accordance with 42 C.F.R. §§ 438.604 and 438.606.

Exhibit B
BUDGET DETAIL AND PAYMENT PROVISIONS

7. System Changes

In the event changes in federal or state law or regulations, including court decisions and interpretations, necessitate a change in either the fiscal or program obligations or operations of the Contractor or the Department, or a change in obligation for the cost of providing covered services the Department and the Contractor agree to negotiate, pursuant to the Welf. & Inst. Code § 14714(c) regarding (a) changes required to remain in compliance with the new law or changes in existing obligations, (b) projected programmatic and fiscal impacts, (c) necessary contract amendments. To the extent that contract amendments are necessary, the parties agree to act to ensure appropriate amendments are made to accommodate any changes required by law or regulation.

8. Administrative Reimbursement

A. The Contractor may submit claims for reimbursement of Medical Administrative Activities (MAA) pursuant to Welf. & Inst. Code § 14132.47. The Contractor shall not submit claims for MAA unless it has submitted a claiming plan to the Department which was approved by the Department and is effective during the quarter in which the costs being claimed were incurred. In addition, the Contractor shall not submit claims for reimbursements of MAA that are not consistent with the Contractor's approved MAA claiming plan. The Contractor shall not use the relative value methodology to report its MAA costs on the year-end cost report. Rather, the Contractor shall calculate and report MAA units on the cost report by multiplying the amount of time (minutes, hours, etc.) spent on MAA activities by the salary plus benefits of the staff performing the activity and then allocating indirect administrative and other appropriately allocated costs.

B. Pursuant to the Welf. & Inst. Code § 14711(c), administrative costs shall be claimed separately in a manner consistent with federal Medicaid requirements and the approved Medicaid state plans and waivers and shall be limited to 15 percent of the total actual cost of direct client services. The cost of performing quality assurance and utilization review activities shall be reimbursed separately and shall not be included in administrative costs.

9. Notification of Request for Contract Amendment

In addition to the provisions in Exhibit E, Additional Provisions, both parties agree to notify the other party whenever an amendment to this contract is to be requested so that informal discussion and consultation can occur prior to a formal amendment process.

Exhibit E
ADDITIONAL PROVISIONS

1. Additional Incorporated Exhibits

A. The following additional exhibits are attached, incorporated herein, and made a part hereof by this reference:

1) Exhibit A, Attachment 9	Documentation Requirements	7 page(s)
2) Exhibit A, Attachment 10	Coordination And Continuity Of Care	2 page(s)
3) Exhibit A, Attachment 11	Information Requirements	10 pages
4) Exhibit A, Attachment 12	Beneficiary Problem Resolution	21 pages
5) Exhibit A, Attachment 13	Program Integrity	7 pages
6) Exhibit A, Attachment 14	Reporting Requirements	3 pages
7) Exhibit B	Budget Detail And Payment Provisions	5 pages
8) Exhibit C *	General Terms And Conditions	GTC 04/2017
9) Exhibit D (F)	Special Terms And Conditions (Attached hereto as part of this agreement) (Notwithstanding Provisions 2, 3, 4, 6 ,8, 12, 14, 22, 25, 29, and 30 which do not apply to this agreement.)	26 pages
10) Exhibit E	Additional Provisions (Program Terms And Conditions)	16 pages
11) Exhibit E, Attachment 1	Definitions	4 pages
12) Exhibit E, Attachment 2	Service Definitions	6 pages
13) Exhibit F	HIPAA Business Associate Addendum	27 pages
14) Exhibit F, Attachment B	Information Security Exchange Agreement between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS)	101 pages

2. Amendment Process

Should either party, during the term of this Contract, desire a change or amendment to the terms of this Contract, such changes or amendments shall be proposed in writing to the other party, who will respond in writing as to whether

Exhibit E
ADDITIONAL PROVISIONS

the proposed changes/amendments are accepted or rejected. If accepted and after negotiations are concluded, the agreed upon changes shall be made through the State's official agreement amendment process. No amendment will be considered binding on either party until it is formally approved by both parties and the Department of General Services (DGS), if DGS approval is required.

3. Cancellation/Termination

A. General Provisions

1) As required by, if the Contractor decides not to contract with the Department, does not renew its contract, or is unable to meet the standards set by the Department, the Contractor agrees to inform the Department of this decision in writing. (Welf. & Inst. Code § 14712(c)(1).)

2) If the Contractor is unwilling to contract for the delivery of specialty mental health services or if the Department or Contractor determines that the Contractor is unable to adequately provide specialty mental health services or that the Contractor does not meet the standards the Department deems necessary for a mental health plan, the Department shall ensure that specialty mental health services are provided to Medi-Cal beneficiaries. (Welf. & Inst. Code § 147122(c)(2), (3).)

3) The Department may contract with qualifying individual counties, counties acting jointly, or other qualified entities approved by the Department for the delivery of specialty mental health services in any county that is unable or unwilling to contract with the Department. The Contractor may not subsequently contract to provide specialty mental health services unless the Department elects to contract with the Contractor. (Welf. & Inst. Code § 147122(c)(4).)

4) If the Contractor does not contract with the Department to provide specialty mental health services, the Department will work with the Department of Finance and the Controller to obtain funds from the Contractor in accordance with Government (Govt.) Code 30027.10. (Welf. & Inst. Code § 147122(d).)

A. Contract Renewal

Exhibit E
ADDITIONAL PROVISIONS

1) This contract may be renewed if the Contractor continues to meet the statutory and regulatory requirements governing this contract, as well as the terms and conditions of this contract. Failure to meet these requirements shall be cause for nonrenewal of the contract. (42 C.F.R. § 438.708; Welf. & Inst. Code § 14714(b)(1).) The Department may base the decision to renew on timely completion of a mutually agreed-upon plan of correction of any deficiencies, submissions of required information in a timely manner, and/or other conditions of the contract. (Welf. & Inst. Code § 14714(b)(1).)

2) In the event the contract is not renewed based on the reasons specified in (1), the Department will notify the Department of Finance, the fiscal and policy committees of the Legislature, and the Controller of the amounts to be sequestered from the Mental Health Subaccount, the Mental Health Equity Account, and the Vehicle License Fee Collection Account of the Local Revenue Fund and the Mental Health Account and the Behavioral Health Subaccount of the Local Revenue Fund 2011, and the Controller will sequester those funds in the Behavioral Health Subaccount pursuant to Govt. Code § 30027.10. Upon this sequestration, the Department will use the funds in accordance with Govt. Code § 30027.10. (Welf. & Inst. Code § 14714(b)(3).)

B. Contract Amendment Negotiations

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

Exhibit E
ADDITIONAL PROVISIONS

amendment is approved by the Department of General Services, if necessary.

D. Contract Termination

The Department or the Contractor may terminate this contract in accordance with, and within the given timeframes provided in California Code of Regulations, title 9, section 1810.323.

1) DHCS reserves the right to cancel or terminate this Contract immediately for cause.

2) The term "for cause" shall mean that the Contractor fails to meet the terms, conditions, and/or responsibilities of this Contract.

3) Contract termination or cancellation shall be effective as of the date indicated in DHCS' notification to the Contractor. The notice shall identify any final performance, invoicing or payment requirements.

4) Upon receipt of a notice of termination or cancellation, the Contractor shall take immediate steps to stop performance and to cancel, or if cancelation is not possible reduce, subsequent contract costs.

5) In the event of early termination or cancellation, the Contractor shall be entitled to payment for all allowable costs authorized under this Contract and incurred up to the date of termination or cancellation, including authorized non-cancelable obligations, provided such expenses do not exceed the stated maximum amounts payable.

6) The Department will immediately terminate this Contract if the Department finds that there is an immediate threat to the health and safety of Medi-Cal beneficiaries. Termination of the contract for other reasons will be subject to reasonable notice to the Contractor of the Department's intent to terminate, as well as notification to affected beneficiaries. (Welf. & Inst. Code § 14714(d).)

E. Termination of Obligations

Exhibit E
ADDITIONAL PROVISIONS

1) All obligations to provide covered services under this contract shall automatically terminate on the effective date of any termination of this contract. The Contractor shall be responsible for providing covered services to beneficiaries until the termination or expiration of the contract and shall remain liable for the processing and payment of invoices and statements for covered services provided to beneficiaries prior to such expiration or termination.

2) When Contractor terminates a subcontract with a provider, Contractor shall make a good faith effort to provide notice of this termination, within 15 days, to the persons that Contractor, based on available information, determines have recently been receiving services from that provider.

F. Contract Disputes

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

4. Fulfillment of Obligation

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

5. Additional Provisions

A. Inspection Rights/Record Keeping Requirements

Exhibit E
ADDITIONAL PROVISIONS

1) Provision number seven (Audit and Record Retention) of Exhibit D(F), which is attached hereto as part of this Contract, supplements the following requirements.

2) The Contractor, and subcontractors, shall allow the Department, CMS, the Office of the Inspector General, the Comptroller General of the United States, and other authorized federal and state agencies, or their duly authorized designees, to evaluate Contractor's, and subcontractors', performance under this contract, including the quality, appropriateness, and timeliness of services provided, and to inspect, evaluate, and audit any and all records, documents, and the premises, equipment and facilities maintained by the Contractor and its subcontractors pertaining to such services at any time. Contractor shall allow such inspection, evaluation and audit of its records, documents and facilities, and those of its subcontractors, for 10 years from the term end date of this Contract or in the event the Contractor has been notified that an audit or investigation of this Contract has been commenced, until such time as the matter under audit or investigation has been resolved, including the exhaustion of all legal remedies, whichever is later. (See 42 C.F.R. §§ 438.3(h), 438.230(c)(3)(i-iii).) Records and documents include, but are not limited to all physical and electronic records and documents originated or prepared pursuant to Contractor's or subcontractor's performance under this Contract including working papers, reports, financial records and documents of account, beneficiary records, prescription files, subcontracts, and any other documentation pertaining to covered services and other related services for beneficiaries.

3) The Contractor, and subcontractors, shall retain, all records and documents originated or prepared pursuant to Contractor's or subcontractor's performance under this Contract, including beneficiary grievance and appeal records identified in Attachment 12, Section 2 and the data, information and documentation specified in 42 Code of Federal Regulations parts 438.604, 438.606, 438.608, and 438.610 for a period of no less than 10 years from the term end date of this Contract or in the event the Contractor has been notified that an audit or investigation of this Contract has been commenced, until such time as the matter under audit or investigation has been resolved, including the exhaustion

Exhibit E
ADDITIONAL PROVISIONS

of all legal remedies, whichever is later. (42 C.F.R. § 438.3(u); See also § 438.3(h).) Records and documents include, but are not limited to all physical and electronic records and documents originated or prepared pursuant to Contractor's or subcontractor's performance under this Contract including working papers, reports, financial records and documents of account, beneficiary records, prescription files, subcontracts, and any other documentation pertaining to covered services and other related services for beneficiaries.

B. Notices

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

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

Yolo County Health and Human Services Agency
137 N. Cottonwood Street, Suite 2500
Woodland, CA 95695

C. Nondiscrimination

1) Consistent with the requirements of applicable federal law, such as 42 Code of Federal Regulations, part 438.3(d)(3) and (4), and state law, the Contractor shall not engage in any unlawful discriminatory practices in the admission of beneficiaries, assignments of accommodations, treatment, evaluation, employment of personnel, or in any other respect on the basis of race, color, gender, gender identity, religion, marital status, national origin, age, sexual orientation, or mental or physical handicap or disability.

2) The Contractor shall comply with the provisions of Section 504 of the Rehabilitation Act of 1973, as amended, pertaining to the prohibition of discrimination against qualified handicapped persons in all federally assisted programs or activities, as detailed in regulations signed by the Secretary of Health and Human Services,

Exhibit E
ADDITIONAL PROVISIONS

effective June 2, 1977, and found in the Federal Register, Volume 42, No. 86, dated May 4, 1977.

3) The Contractor shall include the nondiscrimination and compliance provisions of this contract in all subcontracts to perform work under this contract.

4) Notwithstanding other provisions of this section, the Contractor may require a determination of medical necessity pursuant to California Code of Regulations, title 9, sections 1820.205, 1830.205 and/or 1830.210, prior to providing covered services to a beneficiary.

D. Relationship of the Parties

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

E. Waiver of Default

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

6. Duties of the State

Exhibit E
ADDITIONAL PROVISIONS

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

A. Payment for Services

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

B. Reviews

The Department shall conduct reviews of access to and quality of care in Contractor's county at least once every three years and issue reports to the Contractor detailing findings, recommendations, and corrective action, as appropriate, pursuant to California Code of Regulations, title 9, sections 1810.380 and 1810.385. The Department shall also arrange for an annual external quality review of the Contractor as required by 42 Code of Federal Regulations, part 438.350 and California Code of Regulations, title 9, section 1810.380(a)(7).

C. Monitoring for Compliance

When monitoring activities identify areas of non-compliance, the Department shall issue reports to the Contractor detailing findings, recommendations, and corrective action. Cal. Code Reg., tit. 9, § 1810.380. Failure to comply with required corrective action could lead to civil penalties, as appropriate, pursuant to Cal. Code Reg., tit. 9, § 1810.385.

D. The Contractor shall prepare and submit a report to the Department that provides information for the areas set forth in 42 C.F.R. § 438.66(b) and (c) as outlined in Exhibit A, Attachment 14, Section 7, in the manner specified by the Department.

E. If the Contractor has not previously implemented a Mental Health Plan or Contractor will provide or arrange for the provision of covered benefits to new eligibility groups, then the Contractor shall develop an Implementation

Exhibit E
ADDITIONAL PROVISIONS

Plan (as defined in Cal. Code Regs., tit. 9, § 1810.221) that is consistent with the readiness review requirements set forth in 42 Code of Federal Regulations, part 438.66(d)(4), and the requirements of Cal. Code Regs., tit. 9, § 1810.310 (a). (See 42 C.F.R. § 438.66(d)(1), (4).) The Department shall review and either approve, disapprove, or request additional information for each Implementation Plan. Notices of Approval, Notices of Disapproval and requests for additional information shall be forwarded to the Contractor within 60 days of the receipt of the Implementation Plan. (Cal. Code Regs., tit. 9, § 1810.310(b).) A Contractor shall submit proposed changes to its approved Implementation Plan in writing to the Department for review. A Contractor shall submit proposed changes in the policies, processes or procedures that would modify the Contractor's current Implementation Plan prior to implementing the proposed changes.(See Cal. Code Regs., tit. 9, § 1810.310 (b)-(c)).

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

G. <u>Certification of Organizational Provider Sites Owned or Operated by the Contractor</u>

1) The Department shall certify the organizational provider sites that are owned, leased or operated by the Contractor, in accordance with California Code of Regulations, title 9, section 1810.435, and the requirements specified in Exhibit A, Attachment 3, Section 6 of this contract. This certification shall be performed prior to the date on which the Contractor begins to deliver services under this contract at these sites and once every three years after that date, unless the Department determines an earlier date is necessary. The on-site review required by Cal. Code Regs., tit. 9, § 1810.435(e), shall be conducted of any site owned, leased, or operated by the Contractor and used for to deliver covered services to beneficiaries, except that on-site review is not required for public school or satellite sites.

Exhibit E
ADDITIONAL PROVISIONS

2) The Department may allow the Contractor to begin delivering covered services to beneficiaries at a site subject to on-site review by the Department prior to the date of the on-site review, provided the site is operational and has any required fire clearances. The earliest date the Contractor may begin delivering covered services at a site subject to on site review by the Department is the date the Contractor requested certification of the site in accordance with procedures established by the Department, the date the site was operational, or the date a required fire clearance was obtained, whichever date is latest.

3) The Department may allow the Contractor to continue delivering covered services to beneficiaries at a site subject to on-site review by the Department as part of the recertification process prior to the date of the on-site review, provided the site is operational and has all required fire clearances.

4) Nothing in this section precludes the Department from establishing procedures for issuance of separate provider identification numbers for each of the organizational provider sites operated by the Contractor to facilitate the claiming of FFP by the Contractor and the Department's tracking of that information.

H. Excluded Providers

1) If the Department learns that the Contractor has a prohibited affiliation, as described in Attachment 1, Section 2, the Department:

a) Must notify the Secretary of the noncompliance.

b) May continue an existing agreement with the Contractor unless the Secretary directs otherwise.

c) May not renew or otherwise extend the duration of an existing agreement with the Contractor unless the Secretary provides to the State and to Congress a written statement describing compelling reasons that exist for renewing or extending the agreement despite the prohibited affiliations.

d) Nothing in this section must be construed to limit or otherwise affect any remedies available to the U.S. under

Exhibit E
ADDITIONAL PROVISIONS

sections 1128, 1128A or 1128B of the Act. (42 C.F.R. §438.610(d).)

I. Sanctions

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

J. Notification

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

K. Performance Measurement

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

7. State and Federal Law Governing this Contract

A. Contractor agrees to comply with all applicable federal and state law, including the applicable sections of the state plan and waiver, including but not limited to the statutes and regulations incorporated by reference below in Sections C, E, and F, in its provision of services as the Mental Health Plan. Contractor agrees to comply with any changes to these statutes and regulations that may occur during the contract period and any new applicable statutes or regulations. These obligations shall not apply without the need for a Contract amendment(s). To the extent there is a conflict between federal or state law or regulation and a provision in this contract, Contractor shall comply with the federal or state law or regulation and the conflicting Contract provision shall no longer be in effect.

B. Contractor agrees to comply with all existing policy letters issued by the Department. All policy letters issued by the Department subsequent to the effective date of this Contract shall provide clarification of Contractor's obligations pursuant to this Contract, and may include instructions to the Contractor regarding implementation of mandated obligations pursuant to

Exhibit E
ADDITIONAL PROVISIONS

State or federal statutes or regulations, or pursuant to judicial interpretation.

C. Federal law:

1) Title 42 United States Code, to the extent that these requirements are applicable;

2) 42 C.F.R. to the extent that these requirements are applicable;

3) 42 C.F.R. Part 438, Medicaid Managed Care, limited to those provisions that apply to Prepaid Inpatient Health Plans (PIHPs), except for the provisions listed in paragraph D and E, below.

4) 42 C.F.R. § 455 to the extent that these requirements are applicable;

5) Title VI of the Civil Rights Act of 1964

6) Title IX of the Education Amendments of 1972

7) Age Discrimination Act of 1975

8) Rehabilitation Act of 1973

9) Americans with Disabilities Act

10) Section 1557 of the Patient Protection and Affordable Care Act

11) Deficit Reduction Act of 2005;

12) Balanced Budget Act of 1997.

13) The Contractor shall comply with the provisions of the Copeland Anti-Kickback Act, which requires that all contracts and subcontracts in excess of $2000 for construction or repair awarded by the Contractor and its subcontractors shall include a provision for compliance with the Copeland Anti-Kickback Act.

14) The Contractor shall comply with the provisions of the Davis-Bacon Act, as amended, which provides that, when required by Federal Medicaid program legislation, all construction contracts awarded by

Exhibit E
ADDITIONAL PROVISIONS

the Contractor and its subcontractors of more than $2,000 shall include a provision for compliance with the Davis-Bacon Act as supplemented by Department of Labor regulations.

15) The Contractor shall comply with the provisions of the Contract Work Hours and Safety Standards Act, as applicable, which requires that all subcontracts awarded by the Contractor in excess of $2,000 for construction and in excess of $2,500 for other subcontracts that involve the employment of mechanics or laborers shall include a provision for compliance with the Contract Work Hours and Safety Standards Act.

16) Any applicable federal and state laws that pertain to beneficiary rights.

D. The following sections of 42 Code of Federal Regulations, part 438 are inapplicable to this Contract:

1) §438.3(b) Standard Contract Provisions – Entities eligible for comprehensive risk contracts

2) §438.3(c) Standard Contract Provisions - Payment

3) §438.3(g) Standard Contract Provisions - Provider preventable conditions

4) §438.3(o) Standard Contract Provisions - LTSS contract requirements

5) §438.3(p) Standard Contract Provisions – Special rules for HIOs

6) §438.3(s) Standard Contract Provisions – Requirements for MCOs, PIHPs, or PAHPs that provide covered outpatient drugs

7) §438.4 Actuarial Soundness

8) §438.5 Rate Development Standards

9) §438.6 Special Contract Provisions Related to Payment

10) §438.7 Rate Certification Submission

Exhibit E
ADDITIONAL PROVISIONS

11) §438.8 Medical Loss Ratio Standards

12) §438.9 Provisions that Apply to Non-emergency Medical Transportation

13) §438.50 State Plan Requirements

14) §438.52 Choice of MCOs, PIHPs, PAHPs, PCCMs, and PCCM entities

15) §438.56 Disenrollment: requirements and limitations

16) §438.70 Stakeholder engagement when LTSS is delivered through a managed care program

17) 438.74 State Oversight of the Minimum MLR Requirements

18) §438.104 Marketing

19) §438.110 Member advisory committee

20) §438.114 Emergency and Post-Stabilization

21) §438.362 Exemption from External Quality Review

22) §438.700-730 Basis for Imposition of Sanctions

23) §438.802 Basic Requirements

24) §438.810 Expenditures for Enrollment Broker Services

25) §438.816 Expenditures for the beneficiary support system for enrollees using LTSS

E. Specific provisions of 42 Code of Federal Regulations, part 438 relating to the following subjects are inapplicable to this Contract:

1) Long Terms Services and Supports

2) Managed Long Terms Services and Supports

3) Actuarially Sound Capitation Rates

Exhibit E
ADDITIONAL PROVISIONS

4) Medical Loss Ratio

5) Religious or Moral Objections to Delivering Services

6) Family Planning Services

7) Drug Formularies and Covered Outpatient Drugs

F. Pursuant to Welfare & Institutions Code section 14704, a regulation or order concerning Medi-Cal specialty mental health services adopted by the State Department of Mental Health pursuant to Division 5 (commencing with Section 5000), as in effect preceding the effective date of this section, shall remain in effect and shall be fully enforceable, unless and until the readoption, amendment, or repeal of the regulation or order by DHCS, or until it expires by its own terms.

G. State Law:

1) Division 5, Welfare & Institutions Code, to the extent that these requirements are applicable to the services and functions set forth in this contract

2) Welf. & Inst. Code §§ 14680-14685.1

3) Welf. & Inst. Code §§ 14700-14726

4) Chapter 7, Part 3, Division 9, Welf. & Inst. Code, to the extent that these requirements are applicable to the services and functions set forth in this contract

5) Cal. Code Regs., tit. 9, § 1810.100 et. seq. – Medi-Cal Specialty Mental Health Services

6) Cal. Code Regs., tit. 22, §§ 50951 and 50953

7) Cal. Code Regs., tit. 22, §§ 51014.1 and 51014.2

Exhibit E – Attachment 1
DEFINITIONS

1. The following definitions and the definitions contained in California Code of Regulations, title 9, sections 1810.100-1850.535 shall apply in this contract. If there is a conflict between the following definitions and the definitions in California Code of Regulations, title 9, sections 1810.100-1850.535, the definitions below will apply.

   A. "Advance Directives" means a written instruction, such as a living will or durable power of attorney for health care, recognized under State law (whether statutory or as recognized by the courts of the State), relating to the provision of the healthcare when the individual is incapacitated.

   B. "Abuse" means, as the term described in, provider practices that are inconsistent with sound, fiscal, business, or medical practices, and result in an unnecessary cost to the Medi-Cal program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. It also includes beneficiary practices that result in unnecessary cost to the Medi-Cal program. (See 42 C.F.R. §§ 438.2, 455.2)

   C. "Appeal" means a review by the Contractor of an adverse benefit determination.

   D. "Beneficiary" means a Medi-Cal recipient who is currently receiving services from the Contractor.

   E. "Contractor" means Yolo County Health and Human Services Agency.

   F. "Covered Specialty Mental Health Services" are defined in Exhibit E, Attachment 2.

   G. "Department" means the California Department of Health Care Services (DHCS).

   H. "Director" means the Director of DHCS.

   I. "Emergency" means a condition or situation in which an individual has a need for immediate medical attention, or where the potential for such need is perceived by emergency medical personnel or a public safety agency (Health & Safety Code § 1797.07).

   J. "Fraud" means an intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to self or some other person. It includes an act that

Exhibit E – Attachment 1
DEFINITIONS

constitutes fraud under applicable State and Federal law. (42 C.F.R. §§ 438.2, 455.2)

K. "Grievance" means an expression of dissatisfaction about any matter other than adverse benefit determination. Grievances may include, but are not limited to, the quality of care or services provided, and aspects of interpersonal relationships such as rudeness of a provider or employee, or failure to respect the beneficiary's rights regardless of whether remedial action is requested. Grievance includes a beneficiary's right to dispute an extension of time proposed by the Contractor to make an authorization decision. (42 C.F.R. § 438.400)

L. "Habilitative services and devices" help a person keep, learn, or improve skills and functioning for daily living. (45 C.F.R. § 156.115(a)(5)(i))

M. "HHS" means the United States Department of Health and Human Service

N. "Specialist" means a psychiatrist who has a license as a physician and surgeon in this state and shows evidence of having completed the required course of graduate psychiatric education as specified by the American Board of Psychiatry and Neurology in a program of training accredited by the Accreditation Council for Graduate Medical Education, the American Medical Association, or the American Osteopathic Association. (Cal. Code Regs., tit. 9 § 623.)

O. A "Network Provider" means any provider, group of providers, or entity that has a network provider agreement with a Mental Health Plan, or a subcontractor, and receives Medicaid funding directly or indirectly to order, refer or render covered services as a result of the Department's contract with a Mental Health Plan. A network provider is not a subcontractor by virtue of the network provider agreement. (42 C.F.R. § 438.2)

P. "Out-of-network provider" means a provider or group of providers that does not have a network provider agreement with a Mental Health Plan, or with a subcontractor. (A provider may be "out of network" for one Mental Health Plan, but in the network of another Mental Health Plan.)

Q. "Out-of-plan provider" has the same meaning as out-of-network provider.

R. "Provider" means a person or entity who is licensed, certified, or otherwise recognized or authorized under state law governing the healing arts to provide specialty mental health services and who meets the standards for

Exhibit E – Attachment 1
DEFINITIONS

participation in the Medi-Cal program as described in California Code of Regulations, title 9, Division 1, Chapters 10 or 11 and in Division 3, Subdivision 1 of Title 22, beginning with Section 50000. Provider includes but is not limited to licensed mental health professionals, clinics, hospital outpatient departments, certified day treatment facilities, certified residential treatment facilities, skilled nursing facilities, psychiatric health facilities, general acute care hospitals, and acute psychiatric hospitals. The MHP is a provider when direct services are provided to beneficiaries by employees of the Mental Health Plan.

S. "Overpayment" means any payment made to a network provider by a Mental Health Plan to which the provider is not entitled under Title XIX of the Act or any payment to a Mental Health Plan by a State to which the Mental Health Plan is not entitled to under Title XIX of the Act. (42 C.F.R. § 438.2)

T. "Physician Incentive Plans" mean any compensation arrangement to pay a physician or physician group that may directly or indirectly have the effect of reducing or limiting the services provided to any plan enrollee.

U. "PIHP" means Prepaid Inpatient Health Plan. . A Prepaid Inpatient Health Plan is an entity that:

1) Provides medical services to beneficiaries under contract with the Department of Health Care Services, and on the basis of prepaid capitation payments, or other payment arrangement that does not use state plan rates;

2) Provides, arranges for, or otherwise has responsibility for the provision of any inpatient hospital or institutional services for its beneficiaries; and

3) Does not have a comprehensive risk contract. (42 C.F.R. § 438.2)

V. "Rehabilitation" means a recovery or resiliency focused service activity identified to address a mental health need in the client plan. This service activity provides assistance in restoring, improving, and/or preserving a beneficiary's functional, social, communication, or daily living skills to enhance self-sufficiency or self regulation in multiple life domains relevant to the developmental age and needs of the beneficiary. Rehabilitation also includes support resources, and/or medication education. Rehabilitation may be provided to a beneficiary or a group of beneficiaries. (California's

Exhibit E – Attachment 1
DEFINITIONS

Medicaid State Plan, State Plan Amendment 10-016, Attachment 3.1-A, Supplement 3, p. 2a.)

W. "Satellite site" means a site owned, leased or operated by an organizational provider at which specialty mental health services are delivered to beneficiaries fewer than 20 hours per week, or, if located at a multiagency site at which specialty mental health services are delivered by no more than two employees or contractors of the provider.

X. "Subcontract" means an agreement entered into by the Contractor with any of the following:

1) Any other organization or person who agrees to perform any administrative function or service for the Contractor specifically related to securing or fulfilling the Contractor's obligations to the Department under the terms of this contract.

2) "Subcontractor" means an individual or entity that has a contract with an MCO, PIHP, PAHP, or PCCM entity that relates directly or indirectly to the performance of the MCO's, PIHP's, PAHP's, or PCCM entity's obligations under its contract with the State. A network provider is not a subcontractor by virtue of the network provider agreement with the MCO, PIHP, or PAHP. Notwithstanding the foregoing, for purposes of Exhibit D(F) the term "subcontractor" shall include network providers.

Exhibit E – Attachment 2
SERVICE DEFINITIONS

1. The Contractor shall provide, or arrange and pay for, the following medically necessary covered Specialty Mental Health Services to beneficiaries of Yolo County. Services shall be provided based on medical necessity criteria, in accordance with an individualized Client Plan, and approved and authorized according to State of California requirements. Services include:

   A. Mental Health Services Individual or group therapies and interventions are designed to provide a reduction of mental disability and restoration, improvement or maintenance of functioning consistent with the goals of learning, development, independent living, and enhanced self-sufficiency. These services are separate from those provided as components of adult residential services, crisis intervention, crisis stabilization, day rehabilitation, or day treatment intensive. Service activities may include, but are not limited to:

      1) Assessment - A service activity designed to evaluate the current status of mental, emotional, or behavioral health. Assessment includes, but is not limited to, one or more of the following: mental status determination, analysis of the clinical history, analysis of relevant cultural issues and history; diagnosis; and the use of mental health testing procedures.

      2) Plan Development - A service activity that consists of development of client plans, approval of client plans, and/or monitoring and recording of progress.

      3) Therapy - A service activity that is a therapeutic intervention that focuses primarily on symptom reduction as a means to reduce functional impairments. Therapy may be delivered to an individual or group and may include family therapy at which the client is present.

      4) Rehabilitation - A service activity that includes, but is not limited to, assistance, improving, maintaining or restoring functional skills, daily living skills, social and leisure skills, grooming and personal hygiene skills; obtaining support resources; and/or obtaining medication education.

      5) Collateral - A service activity involving a significant support person in the beneficiary's life for the purpose of addressing the mental health needs of the beneficiary in terms of achieving goals of the beneficiary's client plan. Collateral may include, but is not limited

Exhibit E – Attachment 2
SERVICE DEFINITIONS

to, consultation and training of the significant support person(s) to assist in better utilization of mental health services by the client, consultation and training of the significant support person(s) to assist in better understanding of mental illness, and family counseling with the significant support person(s) in achieving the goals of the client plan. The client may or may not be present for this service activity.

B. Medication Support Services include prescribing, administering, dispensing and monitoring of psychiatric medications or biologicals that are necessary to alleviate the symptoms of mental illness. Service activities may include but are not limited to: evaluation of the need for medication; evaluation of clinical effectiveness and side effects; obtaining informed consent; instruction in the use, risks and benefits of, and alternatives for, medication; collateral and plan development related to the delivery of service and/or assessment for the client; prescribing, administering, dispensing and monitoring of psychiatric medications or biologicals; and medication education.

C. Day Treatment Intensive are a structured, multi-disciplinary program of therapy that may be used as an alternative to hospitalization, or to avoid placement in a more restrictive setting, or to maintain the client in a community setting and which provides services to a distinct group of beneficiaries who receive services for a minimum of three hours per day (half-day) or more than four hours per day (full-day). Service activities may include, but are not limited to, assessment, plan development, therapy, rehabilitation and collateral. Collateral addresses the mental health needs of the beneficiary to ensure coordination with significant others and treatment providers.

D. Day Rehabilitation services are a structured program of rehabilitation and therapy with services to improve, maintain or restore personal independence and functioning, consistent with requirements for learning and development and which provides services to a distinct group of beneficiaries who receive services for a minimum of three hours per day (half-day) or more than four hours per day (full-day). Service activities may include, but are not limited to assessment, plan development, therapy, rehabilitation and collateral. Collateral addresses the mental health needs of the beneficiary to ensure coordination with significant others and treatment providers.

Exhibit E – Attachment 2
SERVICE DEFINITIONS

E. Crisis Intervention services last less than 24 hours and are for, or on behalf of, a beneficiary for a condition that requires more timely response than a regularly scheduled visit. Service activities include, but are not limited to, assessment, collateral and therapy. Crisis Intervention services may either be face-to-face or by telephone with the beneficiary or the beneficiary's significant support person and may be provided anywhere in the community.

F. Crisis Stabilization services last less than 24 hours and are for, or on behalf of, a beneficiary for a condition that requires a more timely response than a regularly scheduled visit. Service activities include but are not limited to one or more of the following: assessment, collateral, and therapy. Collateral addresses the mental health needs of the beneficiary to ensure coordination with significant others and treatment providers.

G. Adult Residential Treatment Services are rehabilitative services provided in a non-institutional, residential setting for beneficiaries who would be at risk of hospitalization or other institutional placement if they were not receiving residential treatment services. The services include a wide range of activities and services that support beneficiaries in their effort to restore, maintain, and apply interpersonal and independent living skills and to access community support systems. Service activities may include assessment, plan development, therapy, rehabilitation, and collateral. Collateral addresses the mental health needs of the beneficiary to ensure coordination with significant others and treatment providers.

H. Crisis Residential services provide an alternative to acute psychiatric hospital services for beneficiaries who otherwise would require hospitalization. The CRS programs for adults provide normalized living environments, integrated into residential communities. The services follow a social rehabilitation model that integrates aspects of emergency psychiatric care, psychosocial rehabilitation, milieu therapy, case management and practical social work.

I. Psychiatric Health Facility Services—A Psychiatric Health Facility is a facility licensed under the provisions beginning with Section 77001 of Chapter 9, Division 5, Title 22 of the California Code of Regulations. "Psychiatric Health Facility Services" are therapeutic and/or rehabilitative services provided in a psychiatric health facility on an inpatient basis to beneficiaries who need acute care, which meets the criteria of Section 1820.205 of Chapter 11, Division 1, Title 9 of the California Code of Regulations, and whose physical health needs can be met in an affiliated

Exhibit E – Attachment 2
SERVICE DEFINITIONS

general acute care hospital or in outpatient settings. These services are separate from those categorized as "Psychiatric Inpatient Hospital".

J. Intensive Care Coordination (ICC) is a targeted case management service that facilitates assessment of, care planning for and coordination of services to beneficiaries under age 21 who are eligible for the full scope of Medi-Cal services and who meet medical necessity criteria for this service. ICC service components include: assessing; service planning and implementation; monitoring and adapting; and transition. ICC services are provided through the principles of the Core Practice Model (CPM), including the establishment of the Child and Family Team (CFT) to ensure facilitation of a collaborative relationship among a youth, his/her family and involved child-serving systems. The CFT is comprised of – as appropriate, both formal supports, such as the care coordinator, providers, case managers from child-serving agencies, and natural supports, such as family members, neighbors, friends, and clergy and all ancillary individuals who work together to develop and implement the client plan and are responsible for supporting the child/youth and family in attaining their goals. ICC also provides an ICC coordinator who:

1) Ensures that medically necessary services are accessed, coordinated and delivered in a strength-based, individualized, family/youth driven and culturally and linguistically competent manner and that services and supports are guided by the needs of the child/youth;

2) Facilitates a collaborative relationship among the child/youth, his/her family and systems involved in providing services to the child/youth;

3) Supports the parent/caregiver in meeting their child/youth's needs;

4) Helps establish the CFT and provides ongoing support; and

5) Organizes and matches care across providers and child serving systems to allow the child/youth to be served in his/her community

K. Intensive Home Based Services (IHBS) are individualized, strength-based interventions designed to ameliorate mental health conditions that interfere with a child/youth's functioning and are aimed at helping the child/youth build skills necessary for successful functioning in the home and community and improving the child/youth's family's ability to help the

Exhibit E – Attachment 2
SERVICE DEFINITIONS

child/youth successfully function in the home and community. IHBS services are provided according to an individualized treatment plan developed in accordance with the Core Practice Model (CPM) by the Child and Family Team (CFT) in coordination with the family's overall service plan which may include IHBS. Service activities may include, but are not limited to assessment, plan development, therapy, rehabilitation and collateral. IHBS is provided to beneficiaries under 21 who are eligible for the full scope of Medi-Cal services and who meet medical necessity criteria for this service.

L. Therapeutic Behavioral Services (TBS) are intensive, individualized, short-term outpatient treatment interventions for beneficiaries up to age 21. Individuals receiving these services have serious emotional disturbances (SED), are experiencing a stressful transition or life crisis and need additional short-term, specific support services to accomplish outcomes specified in the written treatment plan.

M. Therapeutic Foster Care (TFC) Services model allows for the provision of short-term, intensive, highly coordinated, trauma informed and individualized SMHS activities (plan development, rehabilitation and collateral) to children and youth up to age 21 who have complex emotional and behavioral needs and who are placed with trained, intensely supervised and supported TFC parents. The TFC parent serves as a key participant in the therapeutic treatment process of the child or youth. The TFC parent will provide trauma informed interventions that are medically necessary for the child or youth. TFC is intended for children and youth who require intensive and frequent mental health support in a family environment. The TFC service model allows for the provision of certain SMHS activities (plan development, rehabilitation and collateral) available under the EPSDT benefit as a home-based alternative to high level care in institutional settings such as group homes and an alternative to Short Term Residential Therapeutic Programs (STRTPs).

N. Psychiatric Inpatient Hospital Psychiatric Inpatient Hospital Services include both acute psychiatric inpatient hospital services and administrative day services. Acute psychiatric inpatient hospital services are provided to beneficiaries for whom the level of care provided in a hospital is medically necessary to diagnose or treat a covered mental illness. Administrative day services are inpatient hospital services provided to beneficiaries who were admitted to the hospital for an acute psychiatric inpatient hospital service and the beneficiary's stay at the hospital must be continued beyond the beneficiary's need for acute

Exhibit E – Attachment 2
SERVICE DEFINITIONS

psychiatric inpatient hospital services due to lack of residential placement options at non-acute residential treatment facilities that meet the needs of the beneficiary.

Psychiatric inpatient hospital services are provided by SD/MC hospitals and FFS/MC hospitals. MHPs claim reimbursement for the cost of psychiatric inpatient hospital services provided by SD/MC hospitals through the SD/MC claiming system. FFS/MC hospitals claim reimbursement for the cost of psychiatric inpatient hospital services through the Fiscal Intermediary. MHPs are responsible for authorization of psychiatric inpatient hospital services reimbursed through either billing system. For SD/MC hospitals, the daily rate includes the cost of any needed professional services. The FFS/MC hospital daily rate does not include professional services, which are billed separately from the FFS/MC inpatient hospital services via the SD/MC claiming system.

O. Targeted Case Management Targeted case management is a service that assists a beneficiary in accessing needed medical, educational, social, prevocational, vocational, rehabilitative, or other community services. The service activities may include, but are not limited to, communication, coordination and referral; monitoring service delivery to ensure beneficiary access to services and the service delivery system; monitoring of the beneficiary's progress, placement services, and plan development. TCM services may be face-to-face or by telephone with the client or significant support persons and may be provided anywhere in the community. Additionally, services may be provided by any person determined by the MHP to be qualified to provide the service, consistent with the scope of practice and state law.

Special Terms and Conditions

(For federally funded service contracts or agreements and grant agreements)

The use of headings or titles throughout this exhibit is for convenience only and shall not be used to interpret or to govern the meaning of any specific term or condition.

The terms "contract", "Contractor" and "Subcontractor" shall also mean, "agreement", "grant", "grant agreement", "Grantee" and "Subgrantee" respectively.

The terms "California Department of Health Care Services", "California Department of Health Services", 'Department of Health Care Services", "Department of Health Services", "CDHCS", "DHCS", "CDHS", and "DHS" shall all have the same meaning and refer to the California State agency that is a party to this Agreement.

This exhibit contains provisions that require strict adherence to various contracting laws and policies. Some provisions herein are conditional and only apply if specified conditions exist (i.e., agreement total exceeds a certain amount; agreement is federally funded, etc.). The provisions herein apply to this Agreement unless the provisions are removed by reference on the face of this Agreement, the provisions are superseded by an alternate provision appearing elsewhere in this Agreement, or the applicable conditions do not exist.

Index of Special Terms and Conditions

1. Federal Equal Opportunity Requirements

(Applicable to all federally funded agreements entered into by the Department of Health Care Services)

a. The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, national origin, physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era. The Contractor will take affirmative action to ensure that qualified applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, national origin, physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era. Such action shall include, but not be limited to the following: employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and career development opportunities and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Federal Government or DHCS, setting forth the provisions of the Equal Opportunity clause, Section 503 of the Rehabilitation Act of 1973 and the affirmative action clause required by the Vietnam Era Veterans' Readjustment Assistance Act of 1974 (38 U.S.C. 4212). Such notices shall state the Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified applicants without discrimination based on their race, color, religion, sex, national origin physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era and the rights of applicants and employees.

b. The Contractor will, in all solicitations or advancements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era.

c. The Contractor will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding a notice, to be provided by the Federal Government or the State, advising the labor union or workers' representative of the Contractor's commitments under the provisions herein and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

d. The Contractor will comply with all provisions of and furnish all information and reports required by Section 503 of the Rehabilitation Act of 1973, as amended, the Vietnam Era Veterans' Readjustment Assistance Act of 1974 (38 U.S.C. 4212) and of the Federal Executive Order No. 11246 as amended, including by Executive Order 11375, 'Amending Executive Order 11246 Relating to Equal Employment Opportunity,' and as supplemented by regulation at 41 CFR part 60, "Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor," and of the rules, regulations, and relevant orders of the Secretary of Labor.

e. The Contractor will furnish all information and reports required by Federal Executive Order No. 11246 as amended, including by Executive Order 11375, 'Amending Executive Order 11246 Relating to Equal Employment Opportunity,' and as supplemented by regulation at 41 CFR part 60, "Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor," and the Rehabilitation Act of 1973, and by the rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to its books, records, and accounts by the State and its designated representatives and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

f. In the event of the Contractor's noncompliance with the requirements of the provisions herein or with any federal rules, regulations, or orders which are referenced herein, this Agreement may be cancelled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further federal and state contracts in accordance with procedures authorized in Federal Executive Order No. 11246 as amended and such other sanctions may be imposed and remedies invoked as provided in Federal Executive Order No. 11246 as amended, including by Executive Order 11375, 'Amending Executive Order 11246 Relating to Equal Employment Opportunity,' and as supplemented by regulation at 41 CFR part 60, "Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor," or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

g. The Contractor will include the provisions of Paragraphs a through g in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to Federal Executive Order No. 11246 as amended, including by Executive Order 11375, 'Amending Executive Order 11246 Relating to Equal Employment Opportunity,' and as supplemented by regulation at 41 CFR part 60, "Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor," or Section 503 of the Rehabilitation Act of 1973 or (38 U.S.C. 4212) of the Vietnam Era Veteran's Readjustment Assistance Act, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the Director of the Office of Federal Contract Compliance Programs or DHCS may direct as a means of enforcing such provisions including sanctions for noncompliance provided, however, that in the event the Contractor becomes involved in, or is threatened with litigation by a subcontractor or vendor as a result of such direction by DHCS, the Contractor may request in writing to DHCS, who, in turn, may request the United States to enter into such litigation to protect the interests of the State and of the United States.

2. Travel and Per Diem Reimbursement

(Applicable if travel and/or per diem expenses are reimbursed with agreement funds.)

Reimbursement for travel and per diem expenses from DHCS under this Agreement shall, unless otherwise specified in this Agreement, be at the rates currently in effect, as established by the California Department of Human Resources (CalHR), for nonrepresented state employees as stipulated in DHCS' Travel Reimbursement Information Exhibit. If the CalHR rates change during the term of the Agreement, the new rates shall apply upon their effective date and no amendment to this Agreement shall be necessary. Exceptions to CalHR rates may be approved by DHCS upon the submission of a statement by the Contractor indicating that such rates are not available to the Contractor. No travel outside the State of California shall be reimbursed without prior authorization from DHCS. Verbal authorization should be confirmed in writing. Written authorization may be in a form including fax or email confirmation.

3. Procurement Rules

(Applicable to agreements in which equipment/property, commodities and/or supplies are furnished by DHCS or expenses for said items are reimbursed by DHCS with state or federal funds provided under the Agreement.)

a. **Equipment/Property definitions**

Wherever the term equipment and/or property is used, the following definitions shall apply:

(1) **Major equipment/property**: A tangible or intangible item having a base unit cost of **$5,000 or more** with a life expectancy of one (1) year or more and is either furnished by DHCS or the cost is reimbursed through this Agreement. Software and videos are examples of intangible items that meet this definition.

(2) **Minor equipment/property**: A tangible item having a base unit cost of **less than $5,000** with a life expectancy of one (1) year or more and is either furnished by DHCS or the cost is reimbursed through this Agreement.

b. **Government and public entities** (including state colleges/universities and auxiliary organizations), whether acting as a contractor and/or subcontractor, may secure all commodities, supplies, equipment and services related to such purchases that are required in performance of this Agreement. Said procurements are subject to Paragraphs d through h of Provision 3. Paragraph c of Provision 3 shall also apply, if equipment/property purchases are delegated to subcontractors that are nonprofit organizations or commercial businesses.

c. **Nonprofit organizations and commercial businesses**, whether acting as a contractor and/or subcontractor, may secure commodities, supplies, equipment/property and services related to such purchases for performance under this Agreement.

(1) Equipment/property purchases shall not exceed $50,000 annually.

To secure equipment/property above the annual maximum limit of $50,000, the Contractor shall

make arrangements through the appropriate DHCS Program Contract Manager, to have all remaining equipment/property purchased through DHCS' Purchasing Unit. The cost of equipment/property purchased by or through DHCS shall be deducted from the funds available in this Agreement. Contractor shall submit to the DHCS Program Contract Manager a list of equipment/property specifications for those items that the State must procure. DHCS may pay the vendor directly for such arranged equipment/property purchases and title to the equipment/property will remain with DHCS. The equipment/property will be delivered to the Contractor's address, as stated on the face of the Agreement, unless the Contractor notifies the DHCS Program Contract Manager, in writing, of an alternate delivery address.

(2) All equipment/property purchases are subject to Paragraphs d through h of Provision 3. Paragraph b of Provision 3 shall also apply, if equipment/property purchases are delegated to subcontractors that are either a government or public entity.

(3) Nonprofit organizations and commercial businesses shall use a procurement system that meets the following standards:

(a) Maintain a code or standard of conduct that shall govern the performance of its officers, employees, or agents engaged in awarding procurement contracts. No employee, officer, or agent shall participate in the selection, award, or administration of a procurement, or bid contract in which, to his or her knowledge, he or she has a financial interest.

(b) Procurements shall be conducted in a manner that provides, to the maximum extent practical, open, and free competition.

(c) Procurements shall be conducted in a manner that provides for all of the following:

[1] Avoid purchasing unnecessary or duplicate items.

[2] Equipment/property solicitations shall be based upon a clear and accurate description of the technical requirements of the goods to be procured.

[3] Take positive steps to utilize small and veteran owned businesses.

d. Unless waived or otherwise stipulated in writing by DHCS, prior written authorization from the appropriate DHCS Program Contract Manager will be required before the Contractor will be reimbursed for any purchase of $5,000 or more for commodities, supplies, equipment/property, and services related to such purchases. The Contractor must provide in its request for authorization all particulars necessary, as specified by DHCS, for evaluating the necessity or desirability of incurring such costs. The term "purchase" excludes the purchase of services from a subcontractor and public utility services at rates established for uniform applicability to the general public.

e. In special circumstances, determined by DHCS (e.g., when DHCS has a need to monitor certain purchases, etc.), DHCS may require prior written authorization and/or the submission of paid vendor receipts for any purchase, regardless of dollar amount. DHCS reserves the right to either deny claims for reimbursement or to request repayment for any Contractor and/or subcontractor purchase that DHCS determines to be unnecessary in carrying out performance under this Agreement.

f. The Contractor and/or subcontractor must maintain a copy or narrative description of the procurement system, guidelines, rules, or regulations that will be used to make purchases under this Agreement. The State reserves the right to request a copy of these documents and to inspect the purchasing practices of the Contractor and/or subcontractor at any time.

g. For all purchases, the Contractor and/or subcontractor must maintain copies of all paid vendor invoices, documents, bids and other information used in vendor selection, for inspection or audit. Justifications supporting the absence of bidding (i.e., sole source purchases) shall also be maintained on file by the Contractor and/or subcontractor for inspection or audit.

h. DHCS may, with cause (e.g., with reasonable suspicion of unnecessary purchases or use of inappropriate purchase practices, etc.), withhold, cancel, modify, or retract the delegated purchase authority granted under Paragraphs b and/or c of Provision 3 by giving the Contractor no less than 30 calendar days written notice.

4. **Equipment/Property Ownership / Inventory / Disposition**

(Applicable to agreements in which equipment/property is furnished by DHCS and/or when said items are purchased or reimbursed by DHCS with state or federal funds provided under the Agreement.)

a. Wherever the term equipment and/or property is used in Provision 4, the definitions in Paragraph a of Provision 3 shall apply.

Unless otherwise stipulated in this Agreement, all equipment and/or property that is purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement shall be considered state equipment and the property of DHCS.

(1) **Reporting of Equipment/Property Receipt** - DHCS requires the reporting, tagging and annual inventorying of all equipment and/or property that is furnished by DHCS or purchased/reimbursed with funds provided through this Agreement.

Upon receipt of equipment and/or property, the Contractor shall report the receipt to the DHCS Program Contract Manager. To report the receipt of said items and to receive property tags, Contractor shall use a form or format designated by DHCS' Asset Management Unit. If the appropriate form (i.e., Contractor Equipment Purchased with DHCS Funds) does not accompany this Agreement, Contractor shall request a copy from the DHCS Program Contract Manager.

(2) **Annual Equipment/Property Inventory** - If the Contractor enters into an agreement with a term of more than twelve months, the Contractor shall submit an annual inventory of state equipment and/or property to the DHCS Program Contract Manager using a form or format designated by DHCS' Asset Management Unit. If an inventory report form (i.e., Inventory/Disposition of DHCS-Funded Equipment) does not accompany this Agreement, Contractor shall request a copy from the DHCS Program Contract Manager. Contractor shall:

(a) Include in the inventory report, equipment and/or property in the Contractor's possession and/or in the possession of a subcontractor (including independent consultants).

(b) Submit the inventory report to DHCS according to the instructions appearing on the inventory form or issued by the DHCS Program Contract Manager.

(c) Contact the DHCS Program Contract Manager to learn how to remove, trade-in, sell, transfer or survey off, from the inventory report, expired equipment and/or property that is no longer wanted, usable or has passed its life expectancy. Instructions will be supplied by either the DHCS Program Contract Manager or DHCS' Asset Management Unit.

b. Title to state equipment and/or property shall not be affected by its incorporation or attachment to any property not owned by the State.

c. Unless otherwise stipulated, DHCS shall be under no obligation to pay the cost of restoration, or rehabilitation of the Contractor's and/or Subcontractor's facility which may be affected by the removal of any state equipment and/or property.

d. The Contractor and/or Subcontractor shall maintain and administer a sound business program for ensuring the proper use, maintenance, repair, protection, insurance and preservation of state equipment and/or property.

(1) In administering this provision, DHCS may require the Contractor and/or Subcontractor to repair or replace, to DHCS' satisfaction, any damaged, lost or stolen state equipment and/or property. In the event of state equipment and/or miscellaneous property theft, Contractor and/or Subcontractor shall immediately file a theft report with the appropriate police agency or the California Highway Patrol and Contractor shall promptly submit one copy of the theft report to the DHCS Program Contract Manager.

e. Unless otherwise stipulated by the Program funding this Agreement, equipment and/or property purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, shall only be used for performance of this Agreement or another DHCS agreement.

f. Within sixty (60) calendar days prior to the termination or end of this Agreement, the Contractor shall provide a final inventory report of equipment and/or property to the DHCS Program Contract Manager and shall, at that time, query DHCS as to the requirements, including the manner and method, of returning state equipment and/or property to DHCS. Final disposition of equipment and/or property shall be at DHCS expense and according to DHCS instructions. Equipment and/or property disposition instructions shall be issued by DHCS immediately after receipt of the final inventory report. At the termination or conclusion of this Agreement, DHCS may at its discretion, authorize the continued use of state equipment and/or property for performance of work under a different DHCS agreement.

g. **Motor Vehicles**

(Applicable only if motor vehicles are purchased/reimbursed with agreement funds or furnished by DHCS under this Agreement.)

(1) If motor vehicles are purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, within thirty (30) calendar days prior to the termination or end of this Agreement, the Contractor and/or Subcontractor shall return such vehicles to DHCS and shall deliver all necessary documents of title or registration to enable the proper transfer of a marketable title to DHCS.

(2) If motor vehicles are purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, the State of California shall be the legal owner of said motor vehicles and the Contractor shall be the registered owner. The Contractor and/or a subcontractor may only use said vehicles for performance and under the terms of this Agreement.

(3) The Contractor and/or Subcontractor agree that all operators of motor vehicles, purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, shall hold a valid State of California driver's license. In the event that ten or more passengers are to be transported in any one vehicle, the operator shall also hold a State of California Class B driver's license.

(4) If any motor vehicle is purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, the Contractor and/or Subcontractor, as applicable, shall provide, maintain, and certify that, at a minimum, the following type and amount of automobile liability insurance is in effect during the term of this Agreement or any extension period during which any vehicle remains in the Contractor's and/or Subcontractor's possession:

Automobile Liability Insurance

(a) The Contractor, by signing this Agreement, hereby certifies that it possesses or will obtain automobile liability insurance in the amount of $1,000,000 per occurrence for bodily injury and property damage combined. Said insurance must be obtained and made effective upon the delivery date of any motor vehicle, purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, to the Contractor and/or Subcontractor.

(b) The Contractor and/or Subcontractor shall, as soon as practical, furnish a copy of the certificate of insurance to the DHCS Program Contract Manager. The certificate of insurance shall identify the DHCS contract or agreement number for which the insurance applies.

(c) The Contractor and/or Subcontractor agree that bodily injury and property damage liability insurance, as required herein, shall remain in effect at all times during the term of this Agreement or until such time as the motor vehicle is returned to DHCS.

(d) The Contractor and/or Subcontractor agree to provide, at least thirty (30) days prior to the expiration date of said insurance coverage, a copy of a new certificate of insurance evidencing continued coverage, as indicated herein, for not less than the remainder of the term of this Agreement, the term of any extension or continuation thereof, or for a period of not less than one (1) year.

(e) The Contractor and/or Subcontractor, if not a self-insured government and/or public entity, must provide evidence, that any required certificates of insurance contain the following provisions:

[1] The insurer will not cancel the insured's coverage without giving thirty (30) calendar days prior written notice to the State (California Department of Health Care Services).

[2] The State of California, its officers, agents, employees, and servants are included as additional insureds, but only with respect to work performed for the State under this Agreement and any extension or continuation of this Agreement.

[3] The insurance carrier shall notify the California Department of Health Care Services (DHCS), in writing, of the Contractor's failure to pay premiums; its cancellation of such policies; or any other substantial change, including, but not limited to, the status, coverage, or scope of the required insurance. Such notices shall contain a reference to each agreement number for which the insurance was obtained.

(f) The Contractor and/or Subcontractor is hereby advised that copies of certificates of insurance may be subject to review and approval by the Department of General Services (DGS), Office of Risk and Insurance Management. The Contractor shall be notified by DHCS, in writing, if this provision is applicable to this Agreement. If DGS approval of the certificate of insurance is required, the Contractor agrees that no work or services shall be performed prior to obtaining said approval.

(g) In the event the Contractor and/or Subcontractor fails to keep insurance coverage, as required herein, in effect at all times during vehicle possession, DHCS may, in addition to any other remedies it may have, terminate this Agreement upon the occurrence of such event.

5. Subcontract Requirements

(Applicable to agreements under which services are to be performed by subcontractors including independent consultants.)

a. Prior written authorization will be required before the Contractor enters into or is reimbursed for any subcontract for services costing $5,000 or more. Except as indicated in Paragraph a(3) herein, when securing subcontracts for services exceeding $5,000, the Contractor shall obtain at least three bids or justify a sole source award.

(1) The Contractor must provide in its request for authorization, all information necessary for evaluating the necessity or desirability of incurring such cost.

(2) DHCS may identify the information needed to fulfill this requirement.

(3) Subcontracts performed by the following entities or for the service types listed below are exempt from the bidding and sole source justification requirements:

(a) A local governmental entity or the federal government,
(b) A State college or State university from any State,
(c) A Joint Powers Authority,
(d) An auxiliary organization of a California State University or a California community college,
(e) A foundation organized to support the Board of Governors of the California Community Colleges,
(f) An auxiliary organization of the Student Aid Commission established under Education Code § 69522,
(g) Firms or individuals proposed for use and approved by DHCS' funding Program via acceptance of an application or proposal for funding or pre/post contract award negotiations,
(h) Entities and/or service types identified as exempt from advertising and competitive bidding in State Contracting Manual Chapter 5 Section 5.80 Subsection B.2. View this publication at the following Internet address: http://www.dgs.ca.gov/ols/Resources/StateContractManual.aspx.

b. DHCS reserves the right to approve or disapprove the selection of subcontractors and with advance written notice, require the substitution of subcontractors and require the Contractor to terminate subcontracts entered into in support of this Agreement.

(1) Upon receipt of a written notice from DHCS requiring the substitution and/or termination of a subcontract, the Contractor shall take steps to ensure the completion of any work in progress and select a replacement, if applicable, within 30 calendar days, unless a longer period is agreed to by DHCS.

c. Actual subcontracts (i.e., written agreement between the Contractor and a subcontractor) of $5,000 or more are subject to the prior review and written approval of DHCS. DHCS may, at its discretion, elect to waive this right. All such waivers shall be confirmed in writing by DHCS.

d. Contractor shall maintain a copy of each subcontract entered into in support of this Agreement and shall, upon request by DHCS, make copies available for approval, inspection, or audit.

e. DHCS assumes no responsibility for the payment of subcontractors used in the performance of this Agreement. Contractor accepts sole responsibility for the payment of subcontractors used in the performance of this Agreement.

f. The Contractor is responsible for all performance requirements under this Agreement even though performance may be carried out through a subcontract.

g. The Contractor shall ensure that all subcontracts for services include provision(s) requiring compliance with applicable terms and conditions specified in this Agreement.

h. The Contractor agrees to include the following clause, relevant to record retention, in all subcontracts for services:

"(*Subcontractor Name*) agrees to maintain and preserve, until three years after termination of (*Agreement Number*) and final payment from DHCS to the Contractor, to permit DHCS or any duly authorized representative, to have access to, examine or audit any pertinent books, documents, papers and records related to this subcontract and to allow interviews of any employees who might reasonably have information related to such records."

i. Unless otherwise stipulated in writing by DHCS, the Contractor shall be the subcontractor's sole point of contact for all matters related to performance and payment under this Agreement.

j. Contractor shall, as applicable, advise all subcontractors of their obligations pursuant to the following numbered provisions of this Exhibit: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 17, 19, 20, 24, 32 and/or other numbered provisions herein that are deemed applicable.

6. Income Restrictions

Unless otherwise stipulated in this Agreement, the Contractor agrees that any refunds, rebates, credits, or other amounts (including any interest thereon) accruing to or received by the Contractor under this Agreement shall be paid by the Contractor to DHCS, to the extent that they are properly allocable to costs for which the Contractor has been reimbursed by DHCS under this Agreement.

7. Audit and Record Retention

(Applicable to agreements in excess of $10,000.)

a. The Contractor and/or Subcontractor shall maintain books, records, documents, and other evidence, accounting procedures and practices, sufficient to properly reflect all direct and indirect costs of whatever nature claimed to have been incurred in the performance of this Agreement, including any matching costs and expenses. The foregoing constitutes "records" for the purpose of this provision.

b. The Contractor's and/or subcontractor's facility or office or such part thereof as may be engaged in the performance of this Agreement and his/her records shall be subject at all reasonable times to inspection, audit, and reproduction.

c. Contractor agrees that DHCS, the Department of General Services, the Bureau of State Audits, or their designated representatives including the Comptroller General of the United States shall have the right to review and to copy any records and supporting documentation pertaining to the performance of this

Agreement. Contractor agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such records. Further, the Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Agreement. (GC 8546.7, CCR Title 2, Section 1896).

d. The Contractor and/or Subcontractor shall preserve and make available his/her records (1) for a period of three years from the date of final payment under this Agreement, and (2) for such longer period, if any, as is required by applicable statute, by any other provision of this Agreement, or by subparagraphs (1) or (2) below.

   (1) If this Agreement is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for a period of three years from the date of any resulting final settlement.

   (2) If any litigation, claim, negotiation, audit, or other action involving the records has been started before the expiration of the three-year period, the records shall be retained until completion of the action and resolution of all issues which arise from it, or until the end of the regular three-year period, whichever is later.

e. The Contractor and/or Subcontractor shall comply with the above requirements and be aware of the penalties for violations of fraud and for obstruction of investigation as set forth in Public Contract Code § 10115.10, if applicable.

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

g. The Contractor shall, if applicable, comply with the Single Audit Act and the audit reporting requirements set forth in OMB Circular A-133.

8. Site Inspection

The State, through any authorized representatives, has the right at all reasonable times to inspect or otherwise evaluate the work performed or being performed hereunder including subcontract supported activities and the premises in which it is being performed. If any inspection or evaluation is made of the premises of the Contractor or Subcontractor, the Contractor shall provide and shall require Subcontractors to provide all reasonable facilities and assistance for the safety and convenience of the authorized representatives in the performance of their duties. All inspections and evaluations shall be performed in such a manner as will not unduly delay the work.

9. Federal Contract Funds

(Applicable only to that portion of an agreement funded in part or whole with federal funds.)

a. It is mutually understood between the parties that this Agreement may have been written before ascertaining the availability of congressional appropriation of funds, for the mutual benefit of both parties, in order to avoid program and fiscal delays which would occur if the Agreement were executed after that determination was made.

b. This agreement is valid and enforceable only if sufficient funds are made available to the State by the United States Government for the fiscal years covered by the term of this Agreement. In addition, this Agreement 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 Agreement in any manner.

c. It is mutually agreed that if the Congress does not appropriate sufficient funds for the program, this Agreement shall be amended to reflect any reduction in funds.

d. DHCS has the option to invalidate or cancel the Agreement with 30-days advance written notice or to amend the Agreement to reflect any reduction in funds.

10. Intellectual Property Rights

a. Ownership

(1) Except where DHCS has agreed in a signed writing to accept a license, DHCS shall be and remain, without additional compensation, the sole owner of any and all rights, title and interest in all Intellectual Property, from the moment of creation, whether or not jointly conceived, that are made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement.

(2) For the purposes of this Agreement, Intellectual Property means recognized protectable rights and interest such as: patents, (whether or not issued) copyrights, trademarks, service marks, applications for any of the foregoing, inventions, trade secrets, trade dress, logos, insignia, color combinations, slogans, moral rights, right of publicity, author's rights, contract and licensing rights, works, mask works, industrial design rights, rights of priority, know how, design flows, methodologies, devices, business processes, developments, innovations, good will and all other legal rights protecting intangible proprietary information as may exist now and/or here after come into existence, and all renewals and extensions, regardless of whether those rights arise under the laws of the United States, or any other state, country or jurisdiction.

(a) For the purposes of the definition of Intellectual Property, "works" means all literary works, writings and printed matter including the medium by which they are recorded or reproduced, photographs, art work, pictorial and graphic representations and works of a similar nature, film, motion pictures, digital images, animation cells, and other audiovisual works including positives and negatives thereof, sound recordings, tapes, educational materials, interactive videos and any other materials or products created, produced, conceptualized and fixed in a tangible medium of expression. It includes preliminary and final products and any materials and information developed for the purposes of producing those final products. Works does not include articles submitted to peer review or reference journals or independent research projects.

(3) In the performance of this Agreement, Contractor will exercise and utilize certain of its Intellectual Property in existence prior to the effective date of this Agreement. In addition, under this Agreement, Contractor may access and utilize certain of DHCS' Intellectual Property in existence prior to the effective date of this Agreement. Except as otherwise set forth herein, Contractor shall not use any of DHCS' Intellectual Property now existing or hereafter existing for any purposes without the prior written permission of DHCS. **Except as otherwise set forth herein, neither the Contractor nor DHCS shall give any ownership interest in or rights to its Intellectual Property to the other Party.** If during the term of this Agreement, Contractor accesses any third-party Intellectual Property that is licensed to DHCS, Contractor agrees to abide by all license and confidentiality restrictions applicable to DHCS in the third-party's license agreement.

(4) Contractor agrees to cooperate with DHCS in establishing or maintaining DHCS' exclusive rights in the Intellectual Property, and in assuring DHCS' sole rights against third parties with respect to the Intellectual Property. If the Contractor enters into any agreements or subcontracts with other parties in order to perform this Agreement, Contractor shall require the terms of the Agreement(s) to include all Intellectual Property provisions. Such terms must include, but are not limited to, the subcontractor assigning and agreeing to assign to DHCS all rights, title and interest in Intellectual Property made, conceived, derived from, or reduced to practice by the subcontractor, Contractor or DHCS and which result directly or indirectly from this Agreement or any subcontract.

(5) Contractor further agrees to assist and cooperate with DHCS in all reasonable respects, and execute all documents and, subject to reasonable availability, give testimony and take all further acts reasonably necessary to acquire, transfer, maintain, and enforce DHCS' Intellectual Property rights and interests.

b. Retained Rights / License Rights

(1) Except for Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement, Contractor shall retain title to all of its Intellectual Property to the extent such Intellectual Property is in existence prior to the effective date of this Agreement. Contractor hereby grants to DHCS, without additional compensation, a permanent, non-exclusive, royalty free, paid-up, worldwide, irrevocable, perpetual, non-terminable license to use, reproduce, manufacture, sell, offer to sell, import, export, modify, publicly and privately display/perform, distribute, and dispose Contractor's Intellectual Property with the right to sublicense through multiple layers, for any purpose whatsoever, to the extent it is incorporated in the Intellectual Property resulting from this Agreement, unless Contractor assigns all rights, title and interest in the Intellectual Property as set forth herein.

(2) Nothing in this provision shall restrict, limit, or otherwise prevent Contractor from using any ideas, concepts, know-how, methodology or techniques related to its performance under this Agreement, provided that Contractor's use does not infringe the patent, copyright, trademark rights, license or other Intellectual Property rights of DHCS or third party, or result in a breach or default of any provisions of this Exhibit or result in a breach of any provisions of law relating to confidentiality.

c. Copyright

(1) Contractor agrees that for purposes of copyright law, all works [as defined in Paragraph a, subparagraph (2)(a) of this provision] of authorship made by or on behalf of Contractor in connection with Contractor's performance of this Agreement shall be deemed "works made for hire". Contractor further agrees that the work of each person utilized by Contractor in connection with the performance of this Agreement will be a "work made for hire," whether that person is an employee of Contractor or that person has entered into an agreement with Contractor to perform the work. Contractor shall enter into a written agreement with any such person that: (i) all work performed for Contractor shall be deemed a "work made for hire" under the Copyright Act and (ii) that person shall assign all right, title, and interest to DHCS to any work product made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement.

(2) All materials, including, but not limited to, visual works or text, reproduced or distributed pursuant to this Agreement that include Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement, shall include DHCS' notice of copyright, which shall read in 3mm or larger typeface: "© *[Enter Current Year e.g., 2010, etc.]*, California Department of Health Care Services. This material may not be reproduced or disseminated without prior written permission from the California Department of Health Care Services." This notice should be placed prominently on the materials and set apart from other matter on the page where it appears. Audio productions shall contain a similar audio notice of copyright.

d. Patent Rights

With respect to inventions made by Contractor in the performance of this Agreement, which did not result from research and development specifically included in the Agreement's scope of work, Contractor hereby grants to DHCS a license as described under Section b of this provision for devices or material incorporating, or made through the use of such inventions. If such inventions result from research and development work specifically included within the Agreement's scope of work, then Contractor agrees to assign to DHCS, without additional compensation, all its right, title and interest in and to such inventions and to assist DHCS in securing United States and foreign patents with respect thereto.

e. Third-Party Intellectual Property

Except as provided herein, Contractor agrees that its performance of this Agreement shall not be dependent upon or include any Intellectual Property of Contractor or third party without first: (i) obtaining DHCS' prior written approval; and (ii) granting to or obtaining for DHCS, without additional compensation, a license, as described in Section b of this provision, for any of Contractor's or third-party's Intellectual Property in existence prior to the effective date of this Agreement. If such a license upon the these terms is unattainable, and DHCS determines that the Intellectual Property should be included in or is required

for Contractor's performance of this Agreement, Contractor shall obtain a license under terms acceptable to DHCS.

f. Warranties

(1) Contractor represents and warrants that:

(a) It is free to enter into and fully perform this Agreement.

(b) It has secured and will secure all rights and licenses necessary for its performance of this Agreement.

(c) Neither Contractor's performance of this Agreement, nor the exercise by either Party of the rights granted in this Agreement, nor any use, reproduction, manufacture, sale, offer to sell, import, export, modification, public and private display/performance, distribution, and disposition of the Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement will infringe upon or violate any Intellectual Property right, non-disclosure obligation, or other proprietary right or interest of any third-party or entity now existing under the laws of, or hereafter existing or issued by, any state, the United States, or any foreign country. There is currently no actual or threatened claim by any such third party based on an alleged violation of any such right by Contractor.

(d) Neither Contractor's performance nor any part of its performance will violate the right of privacy of, or constitute a libel or slander against any person or entity.

(e) It has secured and will secure all rights and licenses necessary for Intellectual Property including, but not limited to, consents, waivers or releases from all authors of music or performances used, and talent (radio, television and motion picture talent), owners of any interest in and to real estate, sites, locations, property or props that may be used or shown.

(f) It has not granted and shall not grant to any person or entity any right that would or might derogate, encumber, or interfere with any of the rights granted to DHCS in this Agreement.

(g) It has appropriate systems and controls in place to ensure that state funds will not be used in the performance of this Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

(h) It has no knowledge of any outstanding claims, licenses or other charges, liens, or encumbrances of any kind or nature whatsoever that could affect in any way Contractor's performance of this Agreement.

(2) DHCS MAKES NO WARRANTY THAT THE INTELLECTUAL PROPERTY RESULTING FROM THIS AGREEMENT DOES NOT INFRINGE UPON ANY PATENT, TRADEMARK, COPYRIGHT OR THE LIKE, NOW EXISTING OR SUBSEQUENTLY ISSUED.

g. Intellectual Property Indemnity

(1) Contractor shall indemnify, defend and hold harmless DHCS and its licensees and assignees, and its officers, directors, employees, agents, representatives, successors, and users of its products, ("Indemnitees") from and against all claims, actions, damages, losses, liabilities (or actions or proceedings with respect to any thereof), whether or not rightful, arising from any and all actions or claims by any third party or expenses related thereto (including, but not limited to, all legal expenses, court costs, and attorney's fees incurred in investigating, preparing, serving as a witness in, or defending against, any such claim, action, or proceeding, commenced or threatened) to which any of the Indemnitees may be subject, whether or not Contractor is a party to any pending or threatened litigation, which arise out of or are related to (i) the incorrectness or breach of any of the representations, warranties, covenants or agreements of Contractor pertaining to Intellectual Property; or (ii) any Intellectual Property infringement, or any other type of actual or alleged infringement claim, arising out of DHCS' use, reproduction, manufacture, sale, offer to sell, distribution, import, export, modification, public and private performance/display, license, and disposition of the Intellectual Property made, conceived, derived from, or reduced to practice by

Contractor or DHCS and which result directly or indirectly from this Agreement. This indemnity obligation shall apply irrespective of whether the infringement claim is based on a patent, trademark or copyright registration that issued after the effective date of this Agreement. DHCS reserves the right to participate in and/or control, at Contractor's expense, any such infringement action brought against DHCS.

(2) Should any Intellectual Property licensed by the Contractor to DHCS under this Agreement become the subject of an Intellectual Property infringement claim, Contractor will exercise its authority reasonably and in good faith to preserve DHCS' right to use the licensed Intellectual Property in accordance with this Agreement at no expense to DHCS. DHCS shall have the right to monitor and appear through its own counsel (at Contractor's expense) in any such claim or action. In the defense or settlement of the claim, Contractor may obtain the right for DHCS to continue using the licensed Intellectual Property; or, replace or modify the licensed Intellectual Property so that the replaced or modified Intellectual Property becomes non-infringing provided that such replacement or modification is functionally equivalent to the original licensed Intellectual Property. If such remedies are not reasonably available, DHCS shall be entitled to a refund of all monies paid under this Agreement, without restriction or limitation of any other rights and remedies available at law or in equity.

(3) Contractor agrees that damages alone would be inadequate to compensate DHCS for breach of any term of this Intellectual Property Exhibit by Contractor. Contractor acknowledges DHCS would suffer irreparable harm in the event of such breach and agrees DHCS shall be entitled to obtain equitable relief, including without limitation an injunction, from a court of competent jurisdiction, without restriction or limitation of any other rights and remedies available at law or in equity.

h. Federal Funding

In any agreement funded in whole or in part by the federal government, DHCS may acquire and maintain the Intellectual Property rights, title, and ownership, which results directly or indirectly from the Agreement; except as provided in 37 Code of Federal Regulations part 401.14; however, the federal government shall have a non-exclusive, nontransferable, irrevocable, paid-up license throughout the world to use, duplicate, or dispose of such Intellectual Property throughout the world in any manner for governmental purposes and to have and permit others to do so.

i. Survival

The provisions set forth herein shall survive any termination or expiration of this Agreement or any project schedule.

11. Air or Water Pollution Requirements

Any federally funded agreement and/or subcontract in excess of $100,000 must comply with the following provisions unless said agreement is exempt under 40 CFR 15.5.

a. Government contractors agree to comply with all applicable standards, orders, or requirements issued under section 306 of the Clean Air Act [42 U.S.C. 1857(h)], section 508 of the Clean Water Act (33 U.S.C. 1368), Executive Order 11738, and Environmental Protection Agency regulations (40 CFR part 15).

b. Institutions of higher education, hospitals, nonprofit organizations and commercial businesses agree to comply with all applicable standards, orders, or requirements issued under the Clean Air Act (42 U.S.C. 7401 et seq.), as amended, and the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), as amended.

12. Prior Approval of Training Seminars, Workshops or Conferences

Contractor shall obtain prior DHCS approval of the location, costs, dates, agenda, instructors, instructional materials, and attendees at any reimbursable training seminar, workshop, or conference conducted pursuant to this Agreement and of any reimbursable publicity or educational materials to be made available for distribution. The Contractor shall acknowledge the support of the State whenever publicizing the work under this Agreement in any media. This provision does not apply to necessary staff meetings or training sessions held for the staff of the Contractor or Subcontractor to conduct routine business matters.

13. Confidentiality of Information

a. The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure names and other identifying information concerning persons either receiving services pursuant to this Agreement or persons whose names or identifying information become available or are disclosed to the Contractor, its employees, agents, or subcontractors as a result of services performed under this Agreement, except for statistical information not identifying any such person.

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

c. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the DHCS Program Contract Manager all requests for disclosure of such identifying information not emanating from the client or person.

d. The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the client, any such identifying information to anyone other than DHCS without prior written authorization from the DHCS Program Contract Manager, except if disclosure is required by State or Federal law.

e. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph.

f. As deemed applicable by DHCS, this provision may be supplemented by additional terms and conditions covering personal health information (PHI) or personal, sensitive, and/or confidential information (PSCI). Said terms and conditions will be outlined in one or more exhibits that will either be attached to this Agreement or incorporated into this Agreement by reference.

14. Documents, Publications and Written Reports

(Applicable to agreements over $5,000 under which publications, written reports and documents are developed or produced. Government Code Section 7550.)

Any document, publication or written report (excluding progress reports, financial reports and normal contractual communications) prepared as a requirement of this Agreement shall contain, in a separate section preceding the main body of the document, the number and dollar amounts of all contracts or agreements and subcontracts relating to the preparation of such document or report, if the total cost for work by nonemployees of the State exceeds $5,000.

15. Dispute Resolution Process

a. A Contractor grievance exists whenever there is a dispute arising from DHCS' action in the administration of an agreement. If there is a dispute or grievance between the Contractor and DHCS, the Contractor must seek resolution using the procedure outlined below.

(1) The Contractor should first informally discuss the problem with the DHCS Program Contract Manager. If the problem cannot be resolved informally, the Contractor shall direct its grievance together with any evidence, in writing, to the program Branch Chief. The grievance shall state the issues in dispute, the legal authority or other basis for the Contractor's position and the remedy sought. The Branch Chief shall render a decision within ten (10) working days after receipt of the written grievance from the Contractor. The Branch Chief shall respond in writing to the Contractor indicating the decision and reasons therefore. If the Contractor disagrees with the Branch Chief's decision, the Contractor may appeal to the second level.

(2) When appealing to the second level, the Contractor must prepare an appeal indicating the reasons for disagreement with Branch Chief's decision. The Contractor shall include with the appeal a copy of the Contractor's original statement of dispute along with any supporting evidence and a copy of the Branch Chief's decision. The appeal shall be addressed to the Deputy Director of the division in which the branch is organized within ten (10) working days from receipt of the Branch Chief's

decision. The Deputy Director of the division in which the branch is organized or his/her designee shall meet with the Contractor to review the issues raised. A written decision signed by the Deputy Director of the division in which the branch is organized or his/her designee shall be directed to the Contractor within twenty (20) working days of receipt of the Contractor's second level appeal.

b. If the Contractor wishes to appeal the decision of the Deputy Director of the division in which the branch is organized or his/her designee, the Contractor shall follow the procedures set forth in Health and Safety Code Section 100171.

c. Unless otherwise stipulated in writing by DHCS, all dispute, grievance and/or appeal correspondence shall be directed to the DHCS Program Contract Manager.

d. There are organizational differences within DHCS' funding programs and the management levels identified in this dispute resolution provision may not apply in every contractual situation. When a grievance is received and organizational differences exist, the Contractor shall be notified in writing by the DHCS Program Contract Manager of the level, name, and/or title of the appropriate management official that is responsible for issuing a decision at a given level.

16. Financial and Compliance Audit Requirements

a. The definitions used in this provision are contained in Section 38040 of the Health and Safety Code, which by this reference is made a part hereof.

b. Direct service contract means a contract or agreement for services contained in local assistance or subvention programs or both (see Health and Safety [H&S] Code Section 38020). Direct service contracts shall not include contracts, agreements, grants, or subventions to other governmental agencies or units of government nor contracts or agreements with regional centers or area agencies on aging (H&S Code Section 38030).

c. The Contractor, as indicated below, agrees to obtain one of the following audits:

(1) ***If the Contractor is a nonprofit organization (as defined in H&S Code Section 38040)*** and receives **$25,000 or more** from any State agency under a direct service contract or agreement; the Contractor agrees to obtain an annual single, organization wide, financial and compliance audit. Said audit shall be conducted according to Generally Accepted Auditing Standards. This audit does not fulfill the audit requirements of Paragraph c(3) below. The audit shall be completed by the 15th day of the fifth month following the end of the Contractor's fiscal year, **and/or**

(2) ***If the Contractor is a nonprofit organization (as defined in H&S Code Section 38040)*** and receives **less than $25,000** per year from any State agency under a direct service contract or agreement, the Contractor agrees to obtain a biennial single, organization wide financial and compliance audit, unless there is evidence of fraud or other violation of state law in connection with this Agreement. This audit does not fulfill the audit requirements of Paragraph c(3) below. The audit shall be completed by the 15th day of the fifth month following the end of the Contractor's fiscal year, **and/or**

(3) ***If the Contractor is a State or Local Government entity or Nonprofit organization (as defined by the Federal Office of Management and Budget [OMB] Circular A-133)*** and expends $500,000 or more in Federal awards, the Contractor agrees to obtain an annual single, organization wide, financial and compliance audit according to the requirements specified in OMB Circular A-133 entitled "Audits of States, Local Governments, and Non-Profit Organizations". An audit conducted pursuant to this provision will fulfill the audit requirements outlined in Paragraphs c(1) and c(2) above. The audit shall be completed by the end of the ninth month following the end of the audit period. The requirements of this provision apply if:

(a) The Contractor is a recipient expending Federal awards received directly from Federal awarding agencies, or

(b) The Contractor is a subrecipient expending Federal awards received from a pass-through entity such as the State, County or community based organization.

(4) If the Contractor submits to DHCS a report of an audit other than an OMB A-133 audit, the Contractor must also submit a certification indicating the Contractor has not expended $500,000 or more in federal funds for the year covered by the audit report.

d. Two copies of the audit report shall be delivered to the DHCS program funding this Agreement. The audit report must identify the Contractor's legal name and the number assigned to this Agreement. The audit report shall be due within 30 days after the completion of the audit. Upon receipt of said audit report, the DHCS Program Contract Manager shall forward the audit report to DHCS' Audits and Investigations Unit if the audit report was submitted under Section 16.c(3), unless the audit report is from a City, County, or Special District within the State of California whereby the report will be retained by the funding program.

e. The cost of the audits described herein may be included in the funding for this Agreement up to the proportionate amount this Agreement represents of the Contractor's total revenue. The DHCS program funding this Agreement must provide advance written approval of the specific amount allowed for said audit expenses.

f. The State or its authorized designee, including the Bureau of State Audits, is responsible for conducting agreement performance audits which are not financial and compliance audits. Performance audits are defined by Generally Accepted Government Auditing Standards.

g. Nothing in this Agreement limits the State's responsibility or authority to enforce State law or regulations, procedures, or reporting requirements arising thereto.

h. Nothing in this provision limits the authority of the State to make audits of this Agreement, provided however, that if independent audits arranged for by the Contractor meet Generally Accepted Governmental Auditing Standards, the State shall rely on those audits and any additional audit work and shall build upon the work already done.

i. The State may, at its option, direct its own auditors to perform either of the audits described above. The Contractor will be given advance written notification, if the State chooses to exercise its option to perform said audits.

j. The Contractor shall include a clause in any agreement the Contractor enters into with the audit firm doing the single organization wide audit to provide access by the State or Federal Government to the working papers of the independent auditor who prepares the single organization wide audit for the Contractor.

k. Federal or state auditors shall have "expanded scope auditing" authority to conduct specific program audits during the same period in which a single organization wide audit is being performed, but the audit report has not been issued. The federal or state auditors shall review and have access to the current audit work being conducted and will not apply any testing or review procedures which have not been satisfied by previous audit work that has been completed.

The term "expanded scope auditing" is applied and defined in the U.S. General Accounting Office (GAO) issued Standards for *Audit of Government Organizations, Programs, Activities and Functions*, better known as the "yellow book".

17. Human Subjects Use Requirements

(Applicable only to federally funded agreements/grants in which performance, directly or through a subcontract/subaward, includes any tests or examination of materials derived from the human body.)

By signing this Agreement, Contractor agrees that if any performance under this Agreement or any subcontract or subagreement includes any tests or examination of materials derived from the human body for the purpose of providing information, diagnosis, prevention, treatment or assessment of disease, impairment, or health of a human being, all locations at which such examinations are performed shall meet the requirements of 42 U.S.C. Section 263a (CLIA) and the regulations thereunder.

18. Novation Requirements

If the Contractor proposes any novation agreement, DHCS shall act upon the proposal within 60 days after receipt of the written proposal. DHCS may review and consider the proposal, consult and negotiate with the Contractor, and accept or reject all or part of the proposal. Acceptance or rejection of the proposal may be made orally within the 60-day period and confirmed in writing within five days of said decision. Upon written acceptance of the proposal, DHCS will initiate an amendment to this Agreement to formally implement the approved proposal.

19. Debarment and Suspension Certification

(Applicable to all agreements funded in part or whole with federal funds.)

a. By signing this Agreement, the Contractor/Grantee agrees to comply with applicable federal suspension and debarment regulations including, but not limited to 7 CFR Part 3017, 45 CFR 76, 40 CFR 32 or 34 CFR 85.

b. By signing this Agreement, the Contractor certifies to the best of its knowledge and belief, that it and its principals:

   (1) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any federal department or agency;

   (2) Have not within a three-year period preceding this application/proposal/agreement been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

   (3) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in Paragraph b(2) herein; and

   (4) Have not within a three-year period preceding this application/proposal/agreement had one or more public transactions (Federal, State or local) terminated for cause or default.

   (5) Shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under federal regulations (i.e., 48 CFR part 9, subpart 9.4), debarred, suspended, declared ineligible, or voluntarily excluded from participation in such transaction, unless authorized by the State.

   (6) Will include a clause entitled, "Debarment and Suspension Certification" that essentially sets forth the provisions herein, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

c. If the Contractor is unable to certify to any of the statements in this certification, the Contractor shall submit an explanation to the DHCS Program Contract Manager.

d. The terms and definitions herein have the meanings set out in the Definitions and Coverage sections of the rules implementing Federal Executive Order 12549.

e. If the Contractor knowingly violates this certification, in addition to other remedies available to the Federal Government, the DHCS may terminate this Agreement for cause or default.

20. Smoke-Free Workplace Certification

(Applicable to federally funded agreements/grants and subcontracts/subawards, that provide health, day care, early childhood development services, education or library services to children under 18 directly or through local governments.)

a. Public Law 103-227, also known as the Pro-Children Act of 1994 (Act), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, day care, early childhood development services, education or library services to children under the age of 18, if the services are funded by federal programs either directly or through state or local governments, by federal grant, contract, loan, or loan guarantee. The law also applies to children's services that are provided in indoor facilities that are constructed, operated, or maintained with such federal funds. The law does not apply to children's services provided in private residences; portions of facilities used for inpatient drug or alcohol treatment; service providers whose sole source of applicable federal funds is Medicare or Medicaid; or facilities where WIC coupons are redeemed.

b. Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to $1,000 for each violation and/or the imposition of an administrative compliance order on the responsible party.

c. By signing this Agreement, Contractor or Grantee certifies that it will comply with the requirements of the Act and will not allow smoking within any portion of any indoor facility used for the provision of services for children as defined by the Act. The prohibitions herein are effective December 26, 1994.

d. Contractor or Grantee further agrees that it will insert this certification into any subawards (subcontracts or subgrants) entered into that provide for children's services as described in the Act.

21. Covenant Against Contingent Fees

(Applicable only to federally funded agreements.)

The Contractor warrants that no person or selling agency has been employed or retained to solicit/secure this Agreement upon an agreement of understanding for a commission, percentage, brokerage, or contingent fee, except *bona fide* employees or *bona fide* established commercial or selling agencies retained by the Contractor for the purpose of securing business. For breach or violation of this warranty, DHCS shall have the right to annul this Agreement without liability or in its discretion to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such commission, percentage, and brokerage or contingent fee.

22. Payment Withholds

(Applicable only if a final report is required by this Agreement. Not applicable to government entities.)

Unless waived or otherwise stipulated in this Agreement, DHCS may, at its discretion, withhold 10 percent (10%) of the face amount of the Agreement, 50 percent (50%) of the final invoice, or $3,000 whichever is greater, until DHCS receives a final report that meets the terms, conditions and/or scope of work requirements of this Agreement.

23. Performance Evaluation

(Not applicable to grant agreements.)

DHCS may, at its discretion, evaluate the performance of the Contractor at the conclusion of this Agreement. If performance is evaluated, the evaluation shall not be a public record and shall remain on file with DHCS. Negative performance evaluations may be considered by DHCS prior to making future contract awards.

24. Officials Not to Benefit

No members of or delegate of Congress or the State Legislature shall be admitted to any share or part of this Agreement, or to any benefit that may arise therefrom. This provision shall not be construed to extend to this Agreement if made with a corporation for its general benefits.

25. Four-Digit Date Compliance

(Applicable to agreements in which Information Technology (IT) services are provided to DHCS or if IT equipment is procured.)

Contractor warrants that it will provide only Four-Digit Date Compliant (as defined below) Deliverables and/or services to the State. "Four Digit Date compliant" Deliverables and services can accurately process, calculate, compare, and sequence date data, including without limitation date data arising out of or relating to leap years and changes in centuries. This warranty and representation is subject to the warranty terms and conditions of this Contract and does not limit the generality of warranty obligations set forth elsewhere herein.

26. Prohibited Use of State Funds for Software

(Applicable to agreements in which computer software is used in performance of the work.)

Contractor certifies that it has appropriate systems and controls in place to ensure that state funds will not be used in the performance of this Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

27. Use of Small, Minority Owned and Women's Businesses

(Applicable to that portion of an agreement that is federally funded and entered into with institutions of higher education, hospitals, nonprofit organizations or commercial businesses.)

Positive efforts shall be made to use small businesses, minority-owned firms and women's business enterprises, whenever possible (i.e., procurement of goods and/or services). Contractors shall take all of the following steps to further this goal.

(1) Ensure that small businesses, minority-owned firms, and women's business enterprises are used to the fullest extent practicable.

(2) Make information on forthcoming purchasing and contracting opportunities available and arrange time frames for purchases and contracts to encourage and facilitate participation by small businesses, minority-owned firms, and women's business enterprises.

(3) Consider in the contract process whether firms competing for larger contracts intend to subcontract with small businesses, minority-owned firms, and women's business enterprises.

(4) Encourage contracting with consortiums of small businesses, minority-owned firms and women's business enterprises when a contract is too large for one of these firms to handle individually.

(5) Use the services and assistance, as appropriate, of such organizations as the Federal Small Business Administration and the U.S. Department of Commerce's Minority Business Development Agency in the solicitation and utilization of small businesses, minority-owned firms and women's business enterprises.

28. Alien Ineligibility Certification

(Applicable to sole proprietors entering federally funded agreements.)

By signing this Agreement, the Contractor certifies that he/she is not an alien that is ineligible for state and local benefits, as defined in Subtitle B of the Personal Responsibility and Work Opportunity Act. (8 U.S.C. 1601, et seq.)

29. Union Organizing

(Applicable only to grant agreements.)

Grantee, by signing this Agreement, hereby acknowledges the applicability of Government Code Sections 16645 through 16649 to this Agreement. Furthermore, Grantee, by signing this Agreement, hereby certifies that:

a. No state funds disbursed by this grant will be used to assist, promote or deter union organizing.

b. Grantee shall account for state funds disbursed for a specific expenditure by this grant, to show those funds were allocated to that expenditure.

c. Grantee shall, where state funds are not designated as described in b herein, allocate, on a pro-rata basis, all disbursements that support the grant program.

d. If Grantee makes expenditures to assist, promote or deter union organizing, Grantee will maintain records sufficient to show that no state funds were used for those expenditures, and that Grantee shall provide those records to the Attorney General upon request.

30. Contract Uniformity (Fringe Benefit Allowability)

(Applicable only to nonprofit organizations.)

Pursuant to the provisions of Article 7 (commencing with Section 100525) of Chapter 3 of Part 1 of Division 101 of the Health and Safety Code, DHCS sets forth the following policies, procedures, and guidelines regarding the reimbursement of fringe benefits.

a. As used herein fringe benefits shall mean an employment benefit given by one's employer to an employee in addition to one's regular or normal wages or salary.

b. As used herein, fringe benefits do not include:

(1) Compensation for personal services paid currently or accrued by the Contractor for services of employees rendered during the term of this Agreement, which is identified as regular or normal salaries and wages, annual leave, vacation, sick leave, holidays, jury duty and/or military leave/training.
(2) Director's and executive committee member's fees.
(3) Incentive awards and/or bonus incentive pay.
(4) Allowances for off-site pay.
(5) Location allowances.
(6) Hardship pay.
(7) Cost-of-living differentials

c. Specific allowable fringe benefits include:

(1) Fringe benefits in the form of employer contributions for the employer's portion of payroll taxes (i.e., FICA, SUI, SDI), employee health plans (i.e., health, dental and vision), unemployment insurance, worker's compensation insurance, and the employer's share of pension/retirement plans, provided they are granted in accordance with established written organization policies and meet all legal and Internal Revenue Service requirements.

d. To be an allowable fringe benefit, the cost must meet the following criteria:

(1) Be necessary and reasonable for the performance of the Agreement.
(2) Be determined in accordance with generally accepted accounting principles.
(3) Be consistent with policies that apply uniformly to all activities of the Contractor.

e. Contractor agrees that all fringe benefits shall be at actual cost.

f. Earned/Accrued Compensation

(1) Compensation for vacation, sick leave and holidays is limited to that amount earned/accrued within the agreement term. Unused vacation, sick leave and holidays earned from periods prior to the agreement term cannot be claimed as allowable costs. See Provision f (3)(a) for an example.

(2) For multiple year agreements, vacation and sick leave compensation, which is earned/accrued but not paid, due to employee(s) not taking time off may be carried over and claimed within the overall term of the multiple years of the Agreement. Holidays cannot be carried over from one agreement year to the next. See Provision f (3)(b) for an example.

(3) For single year agreements, vacation, sick leave and holiday compensation that is earned/accrued but not paid, due to employee(s) not taking time off within the term of the Agreement, cannot be claimed as an allowable cost. See Provision f (3)(c) for an example.

(a) **Example No. 1:**

If an employee, John Doe, earns/accrues three weeks of vacation and twelve days of sick leave each year, then that is the maximum amount that may be claimed during a one year agreement. If John Doe has five weeks of vacation and eighteen days of sick leave at the beginning of an agreement, the Contractor during a one-year budget period may only claim up to three weeks of vacation and twelve days of sick leave as actually used by the employee. Amounts earned/accrued in periods prior to the beginning of the Agreement are not an allowable cost.

(b) **Example No. 2:**

If during a three-year (multiple year) agreement, John Doe does not use his three weeks of vacation in year one, or his three weeks in year two, but he does actually use nine weeks in year three; the Contractor would be allowed to claim all nine weeks paid for in year three. The total compensation over the three-year period cannot exceed 156 weeks (3 x 52 weeks).

(c) **Example No. 3:**

If during a single year agreement, John Doe works fifty weeks and used one week of vacation and one week of sick leave and all fifty-two weeks have been billed to DHCS, the remaining unused two weeks of vacation and seven days of sick leave may not be claimed as an allowable cost.

31. Suspension or Stop Work Notification

a. DHCS may, at any time, issue a notice to suspend performance or stop work under this Agreement. The initial notification may be a verbal or written directive issued by the funding Program's Contract Manager. Upon receipt of said notice, the Contractor is to suspend and/or stop all, or any part, of the work called for by this Agreement.

b. Written confirmation of the suspension or stop work notification with directions as to what work (if not all) is to be suspended and how to proceed will be provided within 30 working days of the verbal notification. The suspension or stop work notification shall remain in effect until further written notice is received from DHCS. The resumption of work (in whole or part) will be at DHCS' discretion and upon receipt of written confirmation.

(1) Upon receipt of a suspension or stop work notification, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize or halt the incurrence of costs allocable to the performance covered by the notification during the period of work suspension or stoppage.

(2) Within 90 days of the issuance of a suspension or stop work notification, DHCS shall either:

(a) Cancel, extend, or modify the suspension or stop work notification; or

(b) Terminate the Agreement as provided for in the Cancellation / Termination clause of the Agreement.

c. If a suspension or stop work notification issued under this clause is canceled or the period of suspension or any extension thereof is modified or expires, the Contractor may resume work only upon written concurrence of funding Program's Contract Manager.

d. If the suspension or stop work notification is cancelled and the Agreement resumes, changes to the services, deliverables, performance dates, and/or contract terms resulting from the suspension or stop work notification shall require an amendment to the Agreement.

e. If a suspension or stop work notification is not canceled and the Agreement is cancelled or terminated pursuant to the provision entitled Cancellation / Termination, DHCS shall allow reasonable costs resulting from the suspension or stop work notification in arriving at the settlement costs.

f. DHCS shall not be liable to the Contractor for loss of profits because of any suspension or stop work notification issued under this clause.

32. Lobbying Restrictions and Disclosure Certification

(Applicable to federally funded agreements in excess of $100,000 per Section 1352 of the 31, U.S.C.)

a. Certification and Disclosure Requirements

(1) Each person (or recipient) who requests or receives a contract or agreement, subcontract, grant, or subgrant, which is subject to Section 1352 of the 31, U.S.C., and which exceeds $100,000 at any tier, shall file a certification (in the form set forth in Attachment 1, consisting of one page, entitled "Certification Regarding Lobbying") that the recipient has not made, and will not make, any payment prohibited by Paragraph b of this provision.

(2) Each recipient shall file a disclosure (in the form set forth in Attachment 2, entitled "Standard Form-LLL 'disclosure of Lobbying Activities'") if such recipient has made or has agreed to make any payment using nonappropriated funds (to include profits from any covered federal action) in connection with a contract, or grant or any extension or amendment of that contract, or grant, which would be prohibited under Paragraph b of this provision if paid for with appropriated funds.

(3) Each recipient shall file a disclosure form at the end of each calendar quarter in which there occurs any event that requires disclosure or that materially affect the accuracy of the information contained in any disclosure form previously filed by such person under Paragraph a(2) herein. An event that materially affects the accuracy of the information reported includes:

(a) A cumulative increase of $25,000 or more in the amount paid or expected to be paid for influencing or attempting to influence a covered federal action;

(b) A change in the person(s) or individuals(s) influencing or attempting to influence a covered federal action; or

(c) A change in the officer(s), employee(s), or member(s) contacted for the purpose of influencing or attempting to influence a covered federal action.

(4) Each person (or recipient) who requests or receives from a person referred to in Paragraph a(1) of this provision a contract or agreement, subcontract, grant or subgrant exceeding $100,000 at any tier under a contract or agreement, or grant shall file a certification, and a disclosure form, if required, to the next tier above.

(5) All disclosure forms (but not certifications) shall be forwarded from tier to tier until received by the person referred to in Paragraph a(1) of this provision. That person shall forward all disclosure forms to DHCS Program Contract Manager.

b. Prohibition

Section 1352 of Title 31, U.S.C., provides in part that no appropriated funds may be expended by the recipient of a federal contract or agreement, grant, loan, or cooperative agreement to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any of the following covered federal actions: the awarding of any federal contract or agreement, the making of any federal grant, the making of any federal loan, entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract or agreement, grant, loan, or cooperative agreement.

Attachment 1
State of California
Department of Health Care Services

CERTIFICATION REGARDING LOBBYING

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the making, awarding or entering into of this Federal contract, Federal grant, or cooperative agreement, and the extension, continuation, renewal, amendment, or modification of this Federal contract, grant, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency of the United States Government, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, or cooperative agreement, the undersigned shall complete and submit Standard Form LLL, "Disclosure of Lobbying Activities" in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontractors, subgrants, and contracts under grants and cooperative agreements) of $100,000 or more, and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S.C., any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Yolo County Health & Human Services Agency Name of Contractor	Oscar Villegas Printed Name of Person Signing for Contractor
17-94627 Contract / Grant Number	 Signature of Person Signing for Contractor
 Date	Yolo County Board of Supervisors, Chair Title

After execution by or on behalf of Contractor, please return to:

California Department of Health Care Services
Mental Health Services Division/Program Policy Unit
Attn: Dee Taylor
1500 Capitol Avenue, MS 2702
P.O. Box Number 997413
Sacramento, CA 95899-7413

DHCS reserves the right to notifiy the contractor in writing of an alternate submission address.

Attachment 2

CERTIFICATION REGARDING LOBBYING

Approved by OMB
0348-0046

Complete this form to disclose lobbying activities pursuant to 31 U.S.C. 1352
(See reverse for public burden disclosure)

1. Type of Federal Action:	2. Status of Federal Action:	3. Report Type:
[ ] a. contract b. grant c. cooperative agreement d. loan e. loan guarantee f. loan insurance	[ ] a. bid/offer/application b. initial award c. post-award	[ ] a. initial filing b. material change For Material Change Only: Year _____ quarter _____ date of last report _____.

4. Name and Address of Reporting Entity:	5. If Reporting Entity in No. 4 is Subawardee, Enter Name and Address of Prime:
☐ Prime ☐ Subawardee Tier ___, if known: Congressional District, If known:	Congressional District, If known:
6. Federal Department/Agency	7. Federal Program Name/Description: CDFA Number, if applicable: _____
8. Federal Action Number, if known:	9. Award Amount, if known: $
10.a. Name and Address of Lobbying Registrant *(If individual, last name, first name, MI)*:	b. Individuals Performing Services *(including address if different from 10a.* *(Last name, First name, MI)*:
11. Information requested through this form is authorized by title 31 U.S.C. section 1352. This disclosure of lobbying activities is a material representation of fact upon which reliance was placed by the tier above when this transaction was made or entered into. This disclosure is required pursuant to 31 U.S.C. 1352. This information will be available for public inspection. Any person that fails to file the required disclosure shall be subject to a not more than $100,000 for each such failure.	Signature: _____ Print Name: _____ Title: _____ Telephone No.: _____ Date: _____

Federal Use Only	Authorized for Local Reproduction Standard Form-LLL (Rev. 7-97)

INSTRUCTIONS FOR COMPLETION OF SF-LLL, DISCLOSURE OF LOBBYING ACTIVITIES

This disclosure form shall be completed by the reporting entity, whether subawardee or prime Federal recipient, at the initiation or receipt of a covered Federal action, or a material change to a previous filing, pursuant to title 31 U.S.C. section 1352. The filing of a form is required for each payment or agreement to make payment to any lobbying entity for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a covered Federal action. Complete all items that apply for both the initial filing and material change report. Refer to the implementing guidance published by the Office of Management and Budget for additional information.

1. Identify the type of covered Federal action for which lobbying activity is and/or has been secured to influence the outcome of a covered Federal action.

2. Identify the status of the covered Federal action.

3. Identify the appropriateclassification of this report. If this is a followup report caused by a material change to the information previously reported, enter the year and quarter in which the change occurred. Enter the date of the last previously submitted report by this reporting entity for this covered Federal action.

4. Enter the full name, address, city, State and zip code of the reporting entity. Include Congressional District, if known. Check the appropriate classification of the reporting entity that designates if itis, or expects to be,a prime or subaward recipient. Identify the tier of the subawardee, e.g., the first subawardee of the prime is the 1st tier. Subawards include but are not limited to subcontracts, subgrants and contract awards under grants.

5. If the organization filing the report in item 4 checks "Subawardee," then enter the full name, address, city, State and zip code of the prime Federal recipient. Include Congressional District, if known.

6. Enter the name of the Federal agency making the award or loan commitment. Include at least one organizationallevel below agency name, if known. For example, Department of Transportation, United States Coast Guard.

7. Enter the Federal program name or description for the covered Federal action (item 1). If known, enter the full Catalog of Federal Domestic Assistance (CFDA) number for grants, cooperative agreements, loans, and loan commitments.

8. Enter the most appropriate Federal identifying number available for the Federal action identified in item 1 (e.g., Request for Proposal (RFP) number; Invitation for Bid (IFB) number; grant announcement number; the contract, grant, or loan award number, the application/proposal control number assigned by the Federal agency). Include prefixes, e.g., "RFP-DE-90-001".

9. For a covered Federal action where there has been an award or loan commitment by the Federal agency, enter the Federal amount of the award/loan commitment for the prime entity identified in item 4 or 5.

10. (a) Enter the full name, address, city, State and zip code of the lobbying registrant under the Lobbying Disclosure Act of 1995 engaged by the reporting entity identified in item 4 to influence the covered Federal action.

    (b) Enter the full names of the individual(s) performing services, and include full address if different from 10 (a). Enter Last Name, First Name, and Middle Initial (MI).

11. The certifying official shall sign and date the form, print his/her name, title, and telephone number.

According to the Paperwork Reduction Act, as amended, no persons are required to respond to a collection of information unless it displays a valid OMB Control Number. The valid OMB control number for this information collection is OMB No. 0348-0046. Public reporting burden for this collection of information is estimated to average 10 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0046), Washington, DC 20503.

EXHIBIT F
Privacy and Information Security Provisions

Part I: HIPAA Business Associate Addendum

1. Recitals

A. A business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ('the HITECH Act"), 42 U.S.C. § 17921 et seq., and their implementing privacy and security regulations at 45 C.F.R. Parts 160 and 164 ("the HIPAA regulations") between Department and Contractor arises only to the extent that Contractor performs functions or activities on behalf of the Department pursuant to this Agreement that are described in the definition of "business associate" in 45 C.F.R. § 160.103, including but not limited to utilization review, quality assurance, or benefit management.

B. The Department wishes to disclose to Contractor certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, to be used or disclosed in the course of providing services and activities as set forth in Section 1.A. of Exhibit F, Part I of this Agreement. This information is hereafter referred to as "Department PHI".

C. To the extent Contractor performs the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit F, Part I of this Agreement, Contractor is the Business Associate of the Department acting on the Department's behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of the Department and creates, receives, maintains, transmits, uses or discloses PHI and ePHI in the provision of such services or in the performance of such functions or activities. The Department and Contractor are each a party to this Agreement and are collectively referred to as the "parties."

D. The purpose of this Part I is to protect the privacy and security of the PHI and ePHI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that the Department must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 C.F.R. Parts 160 and 164 and the HITECH Act.

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

EXHIBIT F
Privacy and Information Security Provisions

2. Definitions

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

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

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

D. Department PHI shall mean Protected Health Information or Electronic Protected Health Information, as defined below, accessed by Contractor in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services on behalf of the Department as specified in Section 1.A. of Exhibit F, Part I of this Agreement. The terms PHI as used in this document shall mean Department PHI.

E. Electronic Health Records hall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. § 17921 and implementing regulations.

F. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 C.F.R. § 160.103.

G. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 C.F.R. § 160.103.

H. Privacy Rule shall mean the HIPAA Regulations that are found at 45 C.F.R. Parts 160 and 164, Subparts A and E.

I. Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 C.F.R. § 160.103 and as defined under HIPAA.

EXHIBIT F
Privacy and Information Security Provisions

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

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

L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Department PHI, or confidential data utilized by Contractor to perform the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit F, Part I of this Agreement; or interference with system operations in an information system that processes, maintains or stores Department PHI.

M. Security Rule shall mean the HIPAA regulations that are found at 45 C.F.R. Parts 160 and 164.

N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. § 17932(h), any guidance issued by the Secretary pursuant to such Act and the HIPAA regulations.

3. Terms of Agreement

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

B. **Specific Use and Disclosure Provisions**. Except as otherwise indicated in this Exhibit F, Part I, Contractor may:

EXHIBIT F
Privacy and Information Security Provisions

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

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

C. **Prohibited Uses and Disclosures**

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

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

D. **Responsibilities of Contractor**

Contractor agrees:

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

2) **Compliance with the HIPAA Security Rule**. To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Department PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of the Department, in compliance with 45 C.F.R. §§ 164.308, 164.310 and 164.312, and to prevent use or disclosure of Department PHI other than as provided for by this Agreement. Contractor shall implement reasonable and appropriate policies and procedures to comply with the standards,

EXHIBIT F
Privacy and Information Security Provisions

implementation specifications and other requirements of 45 C.F.R. § 164, subpart C, in compliance with 45 C.F.R. § 164.316. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Contractor will provide the Department with its current and updated policies upon request.

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

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

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

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

1) **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.

2) **Mitigation of Harmful Effects**. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PHI by Contractor or its subcontractors in violation of the requirements of this Exhibit F, Part I.

3) **Reporting Unauthorized Use or Disclosure**. To report to Department any use or disclosure of Department PHI not provided for by this Exhibit F, Part I of which it becomes aware.

4) **Contractor's Agents and Subcontractors.**

a) To enter into written agreements with any agents, including subcontractors and vendors to whom Contractor provides Department PHI, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Contractor

EXHIBIT F
Privacy and Information Security Provisions

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

b) In accordance with 45 C.F.R. § 164.504(e)(1)(ii), upon Contractor's knowledge of a material breach or violation by its subcontractor of the agreement between Contractor and the subcontractor, Contractor shall:

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

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

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

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

EXHIBIT F
Privacy and Information Security Provisions

a) If Contractor maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Contractor shall provide such information in an electronic format to enable the Department to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. §17935(e).This section shall be effective as of the date that 42 U.S.C. § 17935(e) and its implementing regulations apply to the Department.

9) **Amendment of Department PHI.** To make any amendment(s) to Department PHI that were requested by a patient and that the Department directs or agrees should be made to assure compliance with 45 C.F.R. § 164.526, in the time and manner designated by the Department, with the Contractor being given a minimum of twenty (20) days within which to make the amendment.

10) **Internal Practices.** To make Contractor's internal practices, books and records relating to the use and disclosure of Department PHI available to the Department or to the Secretary, for purposes of determining the Department's compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Contractor, Contractor shall provide written notification to the Department and shall set forth the efforts it made to obtain the information.

11) **Documentation of Disclosures.** To document and make available to the Department or (at the direction of the Department)to an Individual such disclosures of Department PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of such PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 C.F.R. § 164.528 and 42 U.S.C. § 17935(c). If Contractor maintains electronic health records for the Department as of January 1, 2009, Contractor must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Contractor acquires electronic health records for the Department after January 1, 2009, Contractor must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting. This section shall be effective only as of the date that 42 U.S.C. § 17935(c) and its implementing regulations apply to the Department.

1) **Breaches and Security Incidents.** During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and

EXHIBIT F
Privacy and Information Security Provisions

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

a) **Initial Notice to the Department.** (1) To notify the Department **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured PHI in electronic media or in any other media if the PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. (2) To notify the Department **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement or this Exhibit F, Part I, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

b) Notice shall be provided to the Department Program Contract Manager and the Department Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the Department Information Security Officer. Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link:

http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

c) Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI , Contractor shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

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

d) **Investigation and Investigation Report**. To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI . Within 72 hours of

EXHIBIT F
Privacy and Information Security Provisions

the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Department Program Contract Manager and the Department Information Security Officer.

e) **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Department Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, and the HIPAA regulations. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten(10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.

f) **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in 42 U.S.C. § 17932and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured Department PHI involves more than 500 residents of the State of California or its jurisdiction, Contractor shall notify the Secretary of the breach immediately upon discovery of the breach. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

EXHIBIT F
Privacy and Information Security Provisions

g) **Responsibility for Notification of Affected Individuals.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors and notification of the affected individuals is required under state or federal law, Contractor shall bear all costs of such notifications as well as any costs associated with the breach. In addition, the Department reserves the right to require Contractor to notify such affected individuals, which notifications shall comply with the requirements set forth in 42 U.S.C. § 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The Department Program Contract Manager and the Department Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The Department will provide its review and approval expeditiously and without unreasonable delay.

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

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

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

EXHIBIT F
Privacy and Information Security Provisions

a) Provide an opportunity for the Department to cure the breach or end the violation and terminate the Agreement if the Department does not cure the breach or end the violation within the time specified by Contractor; or

b) Immediately terminate the Agreement if the Department has breached a material term of the Exhibit F, Part I and cure is not possible.

14) **Sanctions and/or Penalties**. Contractor understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Contractors may result in the imposition of sanctions and/or penalties on Contractor under HIPAA, the HITECH Act and the HIPAA regulations.

E. **Obligations of the Department**

The Department agrees to:

1) **Permission by Individuals for Use and Disclosure of PHI**. Provide the Contractor with any changes in, or revocation of, permission by an Individual to use or disclose Department PHI, if such changes affect the Contractor's permitted or required uses and disclosures.

2) **Notification of Restrictions**. Notify the Contractor of any restriction to the use or disclosure of Department PHI that the Department has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the Contractor's use or disclosure of PHI.

3) **Requests Conflicting with HIPAA Rules**. Not request the Contractor to use or disclose Department PHI in any manner that would not be permissible under the HIPAA regulations if done by the Department.

4) **Notice of Privacy Practices**. Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 C.F.R. § 164.520, as well as any changes to such notice. Visit the DHCS Privacy Office to view the most current Notice of Privacy Practices at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx or the DHCS website at www.dhcs.ca.gov (select "Privacy in the right column and "Notice of Privacy Practices" on the right side of the page).

F. **Audits, Inspection and Enforcement**

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

EXHIBIT F
Privacy and Information Security Provisions

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

G. **Termination**

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

2) **Termination for Cause**. In accordance with 45 C.F.R. § 164.504(e)(1)(ii), upon the Department's knowledge of a material breach or violation of this Exhibit F, Part I, by Contractor, the Department shall:

a) Provide an opportunity for Contractor to cure the breach or end the violation and terminate this Agreement if Contractor does not cure the breach or end the violation within the time specified by the Department; or

b) Immediately terminate this Agreement if Contractor has breached a material term of this Exhibit F, Part I, and cure is not possible.

EXHIBIT F
Privacy and Information Security Provisions

Part II: Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA

1. Recitals

A. In addition to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the Department is subject to various other legal and contractual requirements with respect to the personal information (PI) and personally identifiable information (PII)it maintains. These include:

1) The California Information Practices Act of 1977 (California Civil Code §§ 1798 et seq.).

2) The Agreement between the Social Security Administration (SSA) and the Department, known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency. The IEA, including the CMPPA, is attached to this Exhibit F as Attachment B and is hereby incorporated in this Agreement.

B. The purpose of this Exhibit F, Part II is to set forth Contractor's privacy and security obligations with respect to PI and PII that Contractor may create, receive, maintain, use, or disclose for or on behalf of Department pursuant to this Agreement. Specifically this Exhibit applies to PI and PII which is not Protected Health Information (PHI) as defined by HIPAA and therefore is not addressed in Exhibit F, Part I of this Agreement, the HIPAA Business Associate Addendum.

C. The IEA Agreement referenced in A.2) above requires the Department to extend its substantive privacy and security terms to subcontractors who receive data provided to DHCS by the Social Security Administration. If Contractor receives data from DHCS that includes data provided to DHCS by the Social Security Administration, Contractor must comply with the following specific sections of the IEA Agreement: E. Security Procedures, F. Contractor/Agent Responsibilities, and G. Safeguarding and Reporting Responsibilities for Personally Identifiable Information ("PII"), and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the Social Security Administration. Contractor must also ensure that any agents, including a subcontractor, to whom it provides DHCS data that includes data provided by the Social Security Administration, agree to the same requirements for privacy and security safeguards for such confidential data that apply to Contractor with respect to such information.

D. The terms used in this Exhibit F, Part II, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and

EXHIBIT F
Privacy and Information Security Provisions

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

2. Definitions

A. "Breach" shall have the meaning given to such term under the IEA and CMPPA. It shall include a "PII loss" as that term is defined in the CMPPA.

B. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code § 1798.29(d).

C. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS).

D. "Department PI" shall mean Personal Information, as defined below, accessed in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services specified in this Agreement on behalf of the Department.

E. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS).

F. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29(e) whose unauthorized access may trigger notification requirements under Civil Code § 1709.29. For purposes of this provision, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

G. "Personally Identifiable Information" (PII) shall have the meaning given to such term in the IEA and CMPPA.

H. "Personal Information" (PI) shall have the meaning given to such term in California Civil Code § 1798.3(a).

I. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production

EXHIBIT F
Privacy and Information Security Provisions

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

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

3. Terms of Agreement

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

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

B. **Responsibilities of Contractor**

Contractor agrees:

1) **Nondisclosure**. Not to use or disclose Department PI or PII other than as permitted or required by this Agreement or as required by applicable state and federal law.

2) **Safeguards**. To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of Section 3, Security, below. Contractor will provide DHCS with its current policies upon request.

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

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

EXHIBIT F
Privacy and Information Security Provisions

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

c) If the data obtained by User(s) from DHCS includes PII, User(s) shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement (IEA), which are attached as Attachment B and are incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide DHCS PII agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information.

4) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PI or PII by Contractor or its subcontractors in violation of this Exhibit F, Part II.

5) **Contractor's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit F, Part II on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of Department PI or PII to the subcontractor.

6) **Availability of Information to DHCS.** To make Department PI and PII available to the Department for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of Department PI and PII. If Contractor receives Department PII, upon request by DHCS, Contractor shall provide DHCS with a list of all employees, contractors and agents who have access to Department PII, including employees, contractors and agents of its subcontractors and agents.

7) **Cooperation with DHCS.** With respect to Department PI, to cooperate with and assist the Department to the extent necessary to ensure the Department's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of Department PI, correction of

EXHIBIT F
Privacy and Information Security Provisions

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

8) **Breaches and Security Incidents**. During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

a) **Initial Notice to the Department**. (1) To notify the Department **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured Department PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving Department PII. (2) To notify the Department **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of Department PI or PII in violation of this Agreement or this Exhibit F, Part I, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

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

c) Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI , Contractor shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

EXHIBIT F
Privacy and Information Security Provisions

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

d) **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI . Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Department Program Contract Manager and the Department Information Security Officer:

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

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

EXHIBIT F
Privacy and Information Security Provisions

are made. The Department will provide its review and approval expeditiously and without unreasonable delay. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

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

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

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

EXHIBIT F
Privacy and Information Security Provisions

Part III: Miscellaneous Terms and Conditions Applicable to Exhibit F

1. Disclaimer

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

2. Amendment

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

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

2) Contractor does not enter into an amendment providing assurances regarding the safeguarding of Department PHI that the Department deems is necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

3. Judicial or Administrative Proceedings

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

4. Assistance in Litigation or Administrative Proceedings

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

EXHIBIT F
Privacy and Information Security Provisions

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

5. No Third-Party Beneficiaries

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

6. Interpretation

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

7. Conflict

In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Contractor must comply within a reasonable period of time with changes to these standards that occur after the effective date of this Agreement.

8. Regulatory References

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

9. Survival

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

10. No Waiver of Obligations

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

11. Audits, Inspection and Enforcement

EXHIBIT F
Privacy and Information Security Provisions

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

12. Due Diligence

Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit F and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit F.

13. Term

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

14. Effect of Termination

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

EXHIBIT F
Privacy and Information Security Provisions

Attachment A
Business Associate Data Security Requirements

1. Personnel Controls

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

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

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

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

2. Technical Security Controls

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

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

EXHIBIT F
Privacy and Information Security Provisions

C. **Minimum Necessary**. Only the minimum necessary amount of Department PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

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

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

F. **Patch Management**. All workstations, laptops and other systems that process and/or store Department PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.

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

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

H. **Data Destruction**. When no longer needed, all Department PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the Department Information Security Office.

EXHIBIT F
Privacy and Information Security Provisions

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

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

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

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

M. **Transmission encryption**. All data transmissions of Department PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing Department PHI can be encrypted. This requirement pertains to any type of Department PHI or PI in motion such as website access, file transfer, and E-Mail.

N. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting Department PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

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

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

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

EXHIBIT F
Privacy and Information Security Provisions

4. Business Continuity / Disaster Recovery Controls

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

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

5. Paper Document Controls

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

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

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

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

EXHIBIT F
Privacy and Information Security Provisions

Mailings which include 500 or more individually identifiable records of Department PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of the Department to use another method is obtained.

INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

A. PURPOSE: The purpose of this Information Exchange Agreement ("IEA") is to establish terms, conditions, and safeguards under which SSA will disclose to the State Agency certain information, records, or data (herein "data") to assist the State Agency in administering certain federally funded, state-administered benefit programs (including state-funded, state supplementary payment programs under Title XVI of the Social Security Act) identified in this IEA. By entering into this IEA, the State Agency agrees to comply with:

- the terms and conditions set forth in the Computer Matching and Privacy Protection Act Agreement ("CMPPA Agreement") attached as **Attachment 1**, governing the State Agency's use of the data disclosed from SSA's Privacy Act System of Records; and
- all other terms and conditions set forth in this IEA and Attachments 2 through 6.

B. PROGRAMS AND DATA EXCHANGE SYSTEMS: (1) The State Agency will use the data received or accessed from SSA under this IEA for the purpose of administering the federally funded, state-administered programs identified in **Table 1** below. In **Table 1**, the State Agency has identified: (a) each federally funded, state-administered program that it administers; and (b) each SSA data exchange system to which the State Agency needs access in order to administer the identified program. The list of SSA's data exchange systems is attached as **Attachment 2**. **Attachment 2** provides a brief explanation of each system, as well as use parameters, as necessary.

TABLE 1

FEDERALLY FUNDED BENEFIT PROGRAMS	
Program	**SSA Data Exchange System(s)**
☒ Medicaid	BENDEX/SDX/SVES IV/SOLQ/SVES-1-Citizenship/Quarters of Coverage/PUPS
☐ Temporary Assistance to Needy Families (TANF)	
☐ Supplemental Nutrition Assistance Program (SNAP- formally Food Stamps)	
☐ Unemployment Compensation	
☐ State Child Support Agency	
☐ Low-Income Home Energy Assistance Program (LI-HEAP)	
☐ Workers Compensation	
☐ Vocational Rehabilitation Services	

☐ Foster Care (IV-E)	
☒ State Children's Health Insurance Program (CHIP)	BENDEX/SDX/SVES IV,SVES-1 Citizenship
☐ Women, Infants and Children (W.I.C.)	
☒ Medicare Savings Programs (MSP)	LIS File
☒ Medicare 1144 (Outreach)	Medicare 1144 Outreach File
☒ *Other Federally Funded, State-Administered Programs (List Below)*	
Program	**SSA Data Exchange System(s)**
Medi-Cal Access Program (MCAP)	BENDEX/SDX/SVES IV

(2) The State Agency will use each identified data exchange system ***only*** for the purpose of administering the specific program for which access to the data exchange system is provided. SSA data exchange systems are protected by the Privacy Act and Federal law prohibits the use of SSA's data for any purpose other than the purpose of administering the specific program for which such data is disclosed. In particular, the State Agency will:

a) use the **tax return data** disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a program listed in 26 U.S.C. § 6103(l)(7) and (8).

b) use **citizenship status data** disclosed by SSA only to determine entitlement of *new applicants* to: (a) the Medicaid program and CHIP pursuant to the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA to receive the *SSA Data Set* through the Centers for Medicare & Medicaid Services' (CMS) Federal Data Services Hub (Hub).

Applicants for Social Security numbers (SSN) report their citizenship data at the time they apply for their SSNs; there is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files a claim for benefits.

C. **PROGRAM QUESTIONNAIRE:** Prior to signing this IEA, the State Agency will complete and submit to SSA a program questionnaire for each of the federally funded, state-administered programs checked in **Table 1** above. SSA will not disclose any data under this IEA until it has received and approved the completed program questionnaire for each of the programs identified in **Table 1** above.

D. TRANSFER OF DATA: SSA will transmit the data to the State Agency under this IEA using the data transmission method identified in **Table 2** below:

TABLE 2

TRANSFER OF DATA
☐ Data will be transmitted directly between SSA and the State Agency.
☒ Data will be transmitted directly between SSA and The California Office of Technology (State Transmission/Transfer Component ("STC")) by File Transfer Management System (FTMS), a secure mechanism approved by SSA. The STC will serve as the conduit between SSA and the State Agency pursuant to the State STC Agreement.
☐ Data will be transmitted directly between SSA and CMS' Hub by a secure method of transfer approved by SSA. CMS will transmit the *SSA Data Set* between SSA and the State Agency pursuant to an agreement between SSA and CMS regarding the use of the Hub.
☐ Data will be transmitted [*select one:* directly between SSA and the Interstate Connection Network ("ICON") *or* through the [name of STC Agency/Vendor] as the conduit between SSA and the Interstate Connection Network ("ICON")]. ICON is a wide area telecommunications network connecting state agencies that administer the state unemployment insurance laws. When receiving data through ICON, the State Agency will comply with the "Systems Security Requirements for SSA Web Access to SSA Information Through the ICON," attached as **Attachment 3**.

E. SECURITY PROCEDURES: The State Agency will comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), and related National Institute of Standards and Technology guidelines. In addition, the State Agency will comply with SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," attached as **Attachment 4**, as well as the Security Certification Requirements for use of the *SSA Data Set* transmitted via CMS' Hub, attached as **Attachment 5**. The SSA security controls identified under **Attachment 4** of this IEA prevail for all SSA data received by the State Agency, as identified in Table 1 of this IEA. For any tax return data, the State Agency will also comply with the "Tax Information Security Guidelines for Federal, State and Local Agencies," Publication 1075, published by the Secretary of the Treasury and available at the following Internal Revenue Service (IRS) website: http://www.irs.gov/pub/irs-pdf/p1075.pdf. This IRS Publication 1075 is incorporated by reference into this IEA.

F. STATE AGENCY'S RESPONSIBILITIES: The State Agency will not direct individuals to SSA field offices to obtain data that the State Agency is authorized to receive under this IEA in accordance with Table 1. Where disparities exist between individual-supplied data and SSA's data, the State Agency will take the following steps before referring the individual to an SSA field office:

- Check its records to be sure that the data of the original submission has not changed (e.g., last name recently changed);
- Contact the individual to verify the data submitted is accurate; and,
- Consult with the SSA Regional Office Contact to discuss options before advising individuals to contact SSA for resolution. The Regional Office Contact will inform the State Agency of the current protocol through which the individual should contact SSA, i.e., visiting the field office, calling the national network service number, or creating an online account via *my* Social Security.

G. **CONTRACTOR/AGENT RESPONSIBILITIES:** The State Agency will restrict access to the data obtained from SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this IEA. At SSA's request, the State Agency will obtain from each of its contractors and agents a current list of the employees of its contractors and agents who have access to SSA data disclosed under this IEA. The State Agency will require its contractors, agents, and all employees of such contractors or agents with authorized access to the SSA data disclosed under this IEA, to comply with the terms and conditions set forth in this IEA, and not to duplicate, disseminate, or disclose such data without obtaining SSA's prior written approval. In addition, the State Agency will comply with the limitations on use, duplication, and redisclosure of SSA data set forth in Section IX. of the CMPPA Agreement, especially with respect to its contractors and agents.

H. **SAFEGUARDING AND REPORTING RESPONSIBILITIES FOR PERSONALLY IDENTIFIABLE INFORMATION ("PII"):**

1. The State Agency will ensure that its employees, contractors, and agents:
   a. properly safeguard PII furnished by SSA under this IEA from loss, theft, or inadvertent disclosure;
   b. understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee, contractor, or agent is at his or her regular duty station;
   c. ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected;
   d. send emails containing PII only if encrypted or if to and from addresses that are secure; and
   e. limit disclosure of the information and details relating to a PII loss only to those with a need to know.

2. If an employee of the State Agency or an employee of the State Agency's contractor or agent becomes aware of suspected or actual loss of PII, he or she must immediately contact the State Agency official responsible for Systems Security designated below or his or her delegate. That State Agency official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact identified below. If, for any reason, the responsible State Agency official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center at 1-877-697-4889. The responsible State Agency official or delegate will use the worksheet, attached as **Attachment 6**, to quickly gather and

organize information about the incident. The responsible State Agency official or delegate must provide to SSA timely updates as any additional information about the loss of PII becomes available.

3. SSA will make the necessary contact within SSA to file a formal report in accordance with SSA procedures. SSA will notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of PII related to a data exchange under this IEA occurs.

4. If the State Agency experiences a loss or breach of data, it will determine whether or not to provide notice to individuals whose data has been lost or breached and bear any costs associated with the notice or any mitigation.

I. POINTS OF CONTACT:

FOR SSA

San Francisco Regional Office:
Nancy Borjon
Data Exchange Coordinator
Frank Hagel Federal Building
1221 Nevin Avenue
Richmond, CA 94801
Phone: (510) 970-8256
Fax: (510) 970-8101
Email: Nancy.Borjon@ssa.gov

Data Exchange Issues:
Sarah Reagan
Government Information Specialist
Office of the General Counsel
Office of Privacy and Disclosure
617 Altmeyer
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-9127
Fax: (410) 594-0115
Email: Sarah.Reagan@ssa.gov

Program and Policy Issues:
Michael Wilkins
State Liaison Program Manager
Office of Retirement and Disability Policy
Office of Data Exchange and Policy Publications
Office of Data Exchange
3609 Annex Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 966-4965
Fax: (410) 966-4054
Email: Michael.Wilkins@ssa.gov

Systems Security Issues:
Sean Hagan, Acting Director
Division of Compliance and Assessments
Office of Information Security
Office of Systems
Social Security Administration
3829 Annex Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-4519
Fax: (410) 597-0845
Email: Sean.Hagan@ssa.gov

Systems Issues:
Michelle J. Anderson, Branch Chief
DBIAE/Data Exchange and Verification Branch

Office of Information Technology Business Support
Office of Systems
3-D-1 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-5943
Fax: (410) 966-3147
Email: Michelle.J.Anderson@ssa.gov

FOR STATE AGENCY

Agreement Issues:

Rocky Evans
Chief, Eligibility Administration Section
Program Review Branch
Medi-Cal Eligibility Division (MCED)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 319-8434
Fax: (916) 552-9477
Email: Rocky.Evans@dhcs.ca.gov

Technical Issues:

YK Chalamcherla
Chief, Application Development & Support Branch
Enterprise Innovative Technology Services (EITS)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 322-8044
Fax: (916) 440-7065
Email: YK.Chalamcherla@dhcs.ca.gov

Sean Wieland
Chief, Business & Application Integration Section
Enterprise Innovative Technology Services (EITS)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 550-7088
Fax: (916) 440-7065
Email: Sean.Wieland@dhcs.ca.gov

J. **DURATION:** The effective date of this IEA is March 6, 2017. This IEA will remain in effect for as long as: (1) a CMPPA Agreement governing this IEA is in effect between SSA and the State or the State Agency; and (2) the State Agency submits a certification in accordance with Section K. below at least 30 days before the expiration and renewal of such CMPPA Agreement.

K. **CERTIFICATION AND PROGRAM CHANGES:** At least 30 days before the expiration and renewal of the State CMPPA Agreement governing this IEA, the State Agency will certify in writing to SSA that: (1) it is in compliance with the terms and conditions of this IEA; (2) the data exchange processes under this IEA have been and will be conducted without change; and (3) it will, upon SSA's request, provide audit reports or other documents that demonstrate review and oversight activities. If there are substantive changes in any of the programs or data exchange processes listed in this IEA, the parties will modify the IEA in

accordance with Section L. below and the State Agency will submit for SSA's approval new program questionnaires under Section C. above describing such changes prior to using SSA's data to administer such new or changed program.

L. **MODIFICATION:** Modifications to this IEA must be in writing and agreed to by the parties.

M. **TERMINATION:** The parties may terminate this IEA at any time upon mutual written consent. In addition, either party may unilaterally terminate this IEA upon 90 days advance written notice to the other party. Such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow under this IEA, or terminate this IEA, if SSA, in its sole discretion, determines that the State Agency (including its employees, contractors, and agents) has: (1) made an unauthorized use or disclosure of SSA-supplied data; or (2) violated or failed to follow the terms and conditions of this IEA or the CMPPA Agreement.

N. **INTEGRATION:** This IEA, including all attachments, constitutes the entire agreement of the parties with respect to its subject matter. There have been no representations, warranties, or promises made outside of this IEA. This IEA shall take precedence over any other document that may be in conflict with it.

ATTACHMENTS

1 – CMPPA Agreement
2 – SSA Data Exchange Systems
3 – Systems Security Requirements for SSA Web Access to SSA Information Through ICON
4 – Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration
5 – Security Certification Requirements for use of the *SSA Data Set* Transmitted via CMS' Hub
6 – PII Loss Reporting Worksheet

O. AUTHORIZED SIGNATURES: The signatories below warrant and represent that they have competent authority on behalf of their respective agency to enter into the obligations set forth in this IEA.

SOCIAL SECURITY ADMINISTRATION
REGION IX

Grace M. Kim
Regional Commissioner
05/03/2017
Date

THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

Jennifer Kent
Director, California Department of Health Care Services
4/7/17
Date

CERTIFICATION OF COMPLIANCE
FOR
THE INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES (STATE AGENCY)

(State Agency Level)

In accordance with the terms of the Information Exchange Agreement (IEA/F) between SSA and the State Agency, the State Agency, through its authorized representative, hereby certifies that, as of the date of this certification:

1. The State Agency is in compliance with the terms and conditions of the IEA/F;

2. The State Agency has conducted the data exchange processes under the IEA/F without change, except as modified in accordance with the IEA/F;

3. The State Agency will continue to conduct the data exchange processes under the IEA/F without change, except as may be modified in accordance with the IEA/F;

4. Upon SSA's request, the State Agency will provide audit reports or other documents that demonstrate compliance with the review and oversight activities required under the IEA/F and the governing Computer Matching and Privacy Protection Act Agreement; and

5. In compliance with the requirements of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," (last updated July 2015) Attachment 4 to the IEA/F, as periodically updated by SSA, the State Agency has not made any changes in the following areas that could potentially affect the security of SSA data:

    - General System Security Design and Operating Environment
    - System Access Control
    - Automated Audit Trail
    - Monitoring and Anomaly Detection
    - Management Oversight
    - Data and Communications Security
    - Contractors of Electronic Information Exchange Partners
    - Cloud Service Providers for Electronic Information Exchange Partners

The State Agency will submit an updated Security Design Plan at least 30 days prior to making any changes to the areas listed above and provide updated contractor employee lists before allowing new employees' access to SSA provided data.

6. The State Agency agrees that use of computer technology to transfer the data is more economical, efficient, and faster than using a manual process. As such, the State Agency will continue to utilize data exchange to obtain data it needs to administer the programs for which it is authorized, under the IEA/F. Further, before directing an individual to an SSA field office to obtain data, the State Agency will verify that the information it submitted to SSA via data exchange is correct, and verify with the individual that the information he/she supplied is accurate. The use of electronic data exchange expedites program administration and limits SSA field office traffic.

The signatory below warrants and represents that he or she is a representative of the State Agency duly authorized to make this certification on behalf of the State Agency.

DEPARTMENT OF HEALTH CARE SERVICES OF CALIFORNIA

Jennifer Kent
Director

5/17/17
Date

ATTACHMENT 1

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT

(CMPPA)

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT BETWEEN THE SOCIAL SECURITY ADMINISTRATION AND THE HEALTH AND HUMAN SERVICES AGENCY OF CALIFORNIA

I. Purpose and Legal Authority

A. Purpose

This Computer Matching and Privacy Protection Act (CMPPA) Agreement (Agreement) between the Social Security Administration (SSA) and the Health and Human Services Agency of California (State Agency) sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein as "data") made by SSA to the State Agency that administers federally funded benefit programs, including those under various provisions of the Social Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), as well as the state-funded state supplementary payment programs under Title XVI of the Act. The terms and conditions of this Agreement ensure that SSA makes such disclosures of data, and the State Agency uses such disclosed data, in accordance with the requirements of the Privacy Act of 1974, as amended by the CMPPA of 1988, 5 U.S.C. § 552a.

Under section 1137 of the Act, the State Agency is required to use an income and eligibility verification system to administer specified federally funded benefit programs, *including the state-funded state supplementary payment programs* under Title XVI of the Act. To assist the State Agency in determining entitlement to and eligibility for benefits under those programs, as well as other federally funded benefit programs, SSA discloses certain data about applicants (and in limited circumstances, members of an applicant's household), for state benefits from SSA Privacy Act Systems of Records (SOR) and verifies the Social Security numbers (SSN) of the applicants.

B. Legal Authority

SSA's authority to disclose data and the State Agency's authority to collect, maintain, and use data protected under SSA SORs for specified purposes is:

- Sections 453, 1106(b), and 1137 of the Act (42 U.S.C. §§ 653, 1306(b), and 1320b-7) (income and eligibility verification data);
- 26 U.S.C. § 6103(l)(7) and (8) (tax return data);
- Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 402(x)(3)(B)(iv)) and Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii)) (prisoner data);

- Section 205(r)(3) of the Act (42 U.S.C. § 405(r)(3)) and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2) (death data);
- Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645) (quarters of coverage data);
- Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA), Pub. L. 111-3 (citizenship data); and
- Routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3) (data necessary to administer other programs compatible with SSA programs).

This Agreement further carries out section 1106(a) of the Act (42 U.S.C. § 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the CMPPA, related Office of Management and Budget (OMB) guidelines, the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3541, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); and related National Institute of Standards and Technology (NIST) guidelines, which provide the requirements that the State Agency must follow with regard to use, treatment, and safeguarding of data.

II. Scope

A. The State Agency will comply with the terms and conditions of this Agreement and the Privacy Act, as amended by the CMPPA.

B. The State Agency will execute an Information Exchange Agreement (IEA) with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by the State Agency, the data elements that will be disclosed, and the data protection requirements implemented to assist the State Agency in the administration of those programs.

C. The State Agency will use the SSA data governed by this Agreement to determine entitlement and eligibility of individuals for one or more of the following programs, which are specifically identified in the IEA:

1. Temporary Assistance to Needy Families (TANF) program under Part A of Title IV of the Act;
2. Medicaid provided under an approved State plan or an approved waiver under Title XIX of the Act;
3. State Children's Health Insurance Program (CHIP) under Title XXI of the Act, as amended by the Children's Health Insurance Program *Reauthorization Act of 2009*;

4. Supplemental Nutritional Assistance Program (SNAP) under the Food Stamp Act of 1977 (7 U.S.C. § 2011, et seq.);
5. Women, Infants and Children Program (WIC) under the Child Nutrition Act of 1966 (42 U.S.C. § 1771, et seq.);
6. Medicare Savings Programs (MSP) under 42 U.S.C. § 1396a(10)(E);
7. Unemployment Compensation programs provided under a state law described in section 3304 of the Internal Revenue Code of 1954;
8. Low Income Heating and Energy Assistance (LIHEAP or home energy grants) program under 42 U.S.C. § 8621;
9. State-administered supplementary payments of the type described in section 1616(a) of the Act;
10. Programs under a plan approved under Titles I, X, XIV, or XVI of the Act;
11. Foster Care and Adoption Assistance under Title IV of the Act;
12. Child Support Enforcement programs under section 453 of the Act (42 U.S.C. § 653);
13. Other applicable federally funded programs administered by the State Agency under Titles I, IV, X, XIV, XVI, XVIII, XIX, XX, and XXI of the Act; and
14. Any other federally funded programs administered by the State Agency that are compatible with SSA's programs.

D. The State Agency will ensure that SSA data disclosed for the specific purpose of administering a particular federally funded benefit program is used only to administer that program.

III. Justification and Expected Results

A. Justification

This Agreement and related data exchanges with the State Agency are necessary for SSA to assist the State Agency in its administration of federally funded benefit programs by providing the data required to accurately determine entitlement and eligibility of individuals for benefits provided under these programs. SSA uses computer technology to transfer the data because it is more economical, efficient, and faster than using manual processes.

B. Expected Results

The State Agency will use the data provided by SSA to improve public service and program efficiency and integrity. The use of SSA data expedites the application process and ensures that benefits are awarded only to applicants that satisfy the State Agency's program criteria. A cost-benefit analysis for the exchange made under this Agreement is not required in accordance with the determination by the SSA Data Integrity Board (DIB) to waive such analysis pursuant to 5 U.S.C. § 552a(u)(4)(B).

IV. Record Description

A. Systems of Records (SOR)

SSA SORs used for purposes of the subject data exchanges include:

- 60-0058 -- Master Files of SSN Holders and SSN Applications;
- 60-0059 -- Earnings Recording and Self-Employment Income System;
- 60-0090 -- Master Beneficiary Record;
- 60-0103 -- Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB);
- 60-0269 -- Prisoner Update Processing System (PUPS); and
- 60-0321 -- Medicare Part D and Part D Subsidy File.

The State Agency will only use the tax return data contained in **SOR 60-0059** (Earnings Recording and Self-Employment Income System) in accordance with 26 U.S.C. § 6103.

B. Data Elements

Data elements disclosed in computer matching governed by this Agreement are Personally Identifiable Information (PII) from specified SSA SORs, including names, SSNs, addresses, amounts, and other information related to SSA benefits and earnings information. Specific listings of data elements are available at:

http://www.ssa.gov/dataexchange/

C. Number of Records Involved

The maximum number of records involved in this matching activity is the number of records maintained in SSA's SORs listed above in Section IV.A.

V. Notice and Opportunity to Contest Procedures

A. Notice to Applicants

The State Agency will notify all individuals who apply for federally funded, state-administered benefits that any data they provide are subject to verification through computer matching with SSA. The State Agency and SSA will provide such notice through appropriate language printed on application forms or separate handouts.

B. Notice to Beneficiaries/Recipients/Annuitants

The State Agency will provide notice to beneficiaries, recipients, and annuitants under the programs covered by this Agreement informing them of ongoing computer matching with SSA. SSA will provide such notice through publication in the Federal Register and periodic mailings to all beneficiaries, recipients, and annuitants describing SSA's matching activities.

C. Opportunity to Contest

The State Agency will not terminate, suspend, reduce, deny, or take other adverse action against an applicant for or recipient of federally funded, state-administered benefits based on data disclosed by SSA from its SORs until the individual is notified in writing of the potential adverse action and provided an opportunity to contest the planned action. "Adverse action" means any action that results in a termination, suspension, reduction, or final denial of eligibility, payment, or benefit. Such notices will:

1. Inform the individual of the match findings and the opportunity to contest these findings;

2. Give the individual until the expiration of any time period established for the relevant program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond; and

3. Clearly state that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the SSA data are correct and will effectuate the planned action or otherwise make the necessary adjustment to the individual's benefit or entitlement.

VI. Records Accuracy Assessment and Verification Procedures

Pursuant to 5 U.S.C. § 552a(p)(1)(A)(ii), SSA's DIB has determined that the State Agency may use SSA's benefit data without independent verification. SSA has independently assessed the accuracy of its benefits data to be more than 99 percent accurate when the benefit record is created.

Prisoner and death data, some of which is not independently verified by SSA, does not have the same degree of accuracy as SSA's benefit data. Therefore, the State Agency must independently verify these data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

Based on SSA's Office of Quality Review "Fiscal Year 2014 Enumeration Accuracy Report," the SSA Enumeration System database (the Master Files of SSN Holders and SSN Applications System) used for SSN matching is 99 percent accurate for records updated by SSA employees.

Individuals applying for SSNs report their citizenship status at the time they apply for their SSNs. There is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files for a Social Security benefit. The State Agency must independently verify citizenship data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

VII. Disposition and Records Retention of Matched Items

A. The State Agency will retain all data received from SSA to administer programs governed by this Agreement only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.

B. The State Agency may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing the State Agency's retention of records.

C. The State Agency may use any accretions, deletions, or changes to the SSA data governed by this Agreement to update their master files of federally funded, state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing the State Agency's retention of records.

D. The State Agency may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this Agreement.

E. SSA will delete electronic data input files received from the State Agency after it processes the applicable match. SSA will retire its data in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

VIII. Security Procedures

SSA and the State Agency will comply with the security and safeguarding requirements of the Privacy Act, as amended by the CMPPA, related OMB guidelines, FISMA, related NIST guidelines, and the current revision of Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, available at http://www.irs.gov. In addition, SSA

and the State Agency will have in place administrative, technical, and physical safeguards for the matched data and results of such matches. Additional administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency, including SSA's *Electronic Information Exchange Security Requirements and Procedures for State and local Agencies Exchanging Electronic Information with SSA*, as well as specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

SSA has the right to monitor the State Agency's compliance with FISMA, the terms of this Agreement, and the IEA and to make onsite inspections of the State Agency for purposes of auditing compliance, if necessary, during the lifetime of this Agreement or of any extension of this Agreement. This right includes onsite inspection of any entity that receives SSA information from the State Agency under the terms of this Agreement, if SSA determines it is necessary.

IX. Records Usage, Duplication, and Redisclosure Restrictions

A. The State Agency will use and access SSA data and the records created using that data only for the purpose of verifying eligibility for the specific federally funded benefit programs identified in the IEA.

B. The State Agency will comply with the following limitations on use, duplication, and redisclosure of SSA data:

1. The State Agency will not use or redisclose the data disclosed by SSA for any purpose other than to determine eligibility for, or the amount of, benefits under the state-administered income/health maintenance programs identified in this Agreement.

2. The State Agency will not extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs identified in this Agreement. In limited circumstances that are approved by SSA, the State Agency may extract information about an individual other than the applicant/recipient when the applicant/recipient has provided identifying information about the individual and the individual's income or resources affect the applicant's/recipient's eligibility for such program.

3. The State Agency will not disclose to an applicant/recipient information about another individual (i.e., an applicant's household member) without the written consent from the individual to whom the information pertains.

4. The State Agency will use the Federal tax information (FTI) disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to section 1137 programs and child support enforcement

programs in accordance with 26 U.S.C. § 6103(l)(7) and (8). The State Agency receiving FTI will maintain all FTI from IRS in accordance with 26 U.S.C. § 6103(p)(4) and the IRS Publication 1075. Contractors and agents acting on behalf of the State Agency will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103 and the current revision IRS Publication 1075.

5. The State Agency will use the citizenship status data disclosed by SSA only to determine entitlement of new applicants to: (a) the Medicaid program and CHIP pursuant to CHIPRA, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA. The State Agency will further comply with additional terms and conditions regarding use of citizenship data, as set forth in the State Agency's IEA.

6. The State Agency will restrict access to the data disclosed by SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with the purposes identified in this Agreement.

7. The State Agency will enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties whereby such contractor or agent agrees to abide by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement. The State Agency will provide its contractors and agents with copies of this Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing this Agreement, and thereafter at SSA's request, the State Agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

8. If the State Agency is authorized or required – pursuant to an applicable law, regulation, or intra-governmental documentation – to provide SSA data to another State or local government entity for the administration of the federally funded, state-administered programs covered by this Agreement, the State Agency must ensure that the State or local government entity, including its employees, abides by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement and the IEA. At SSA's request, the State Agency will provide copies of any applicable law, regulation, or intra-governmental documentation that authorizes the intra-governmental relationship with the State or local government entity. Upon request from SSA, the State Agency will also establish how it ensures that State or local government entity complies with the terms of this Agreement and the IEA.

9. The State Agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this Agreement

may be subject to civil and criminal sanctions pursuant to applicable Federal statutes.

10. The State Agency will conduct triennial compliance reviews of its contractor(s) and agent(s) no later than three years after the initial approval of the security certification to SSA. The State Agency will share documentation of its recurring compliance reviews with its contractor(s) and agent(s) with SSA. The State Agency will provide documentation to SSA during its scheduled compliance and certification reviews or upon request.

C. The State Agency will not duplicate in a separate file or disseminate, without prior written permission from SSA, the data governed by this Agreement for any purpose other than to determine entitlement to, or eligibility for, federally funded benefits. The State Agency proposing the redisclosure must specify in writing to SSA what data are being disclosed, to whom, and the reasons that justify the redisclosure. SSA will not give permission for such redisclosure unless the redisclosure is required by law or essential to the conduct of the matching program and authorized under a routine use. To the extent SSA approves the requested redisclosure, the State Agency will ensure that any entity receiving the redisclosed data will comply with the procedures and limitations on use, duplication, and redisclosure of SSA data, as well as all administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency including specific guidance on safeguarding and reporting responsibilities for PII, as set forth in this Agreement and the accompanying IEAs.

X. Comptroller General Access

The Comptroller General (the Government Accountability Office) may have access to all records of the State Agency that the Comptroller General deems necessary to monitor and verify compliance with this Agreement in accordance with 5 U.S.C. § 552a(o)(l)(K).

XI. Duration, Modification, and Termination of the Agreement

A. Duration

1. This Agreement is effective from July 1, 2017 (Effective Date) through December 31, 2018 (Expiration Date).

2. In accordance with the CMPPA, SSA will: (a) publish a Computer Matching Notice in the Federal Register at least 30 days prior to the Effective Date; (b) send required notices to the Congressional committees of jurisdiction under 5 U.S.C. § 552a(o)(2)(A)(i) at least 40 days prior to the

Effective Date; and (c) send the required report to OMB at least 40 days prior to the Effective Date.

3. Within 3 months prior the Expiration Date, the SSA DIB may, without additional review, renew this Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:

   - the applicable data exchange will continue without any change; and
   - SSA and the State Agency certify to the DIB in writing that the applicable data exchange has been conducted in compliance with this Agreement.

4. If either SSA or the State Agency does not wish to renew this Agreement, it must notify the other party of its intent not to renew at least 3 months prior to the Expiration Date.

B. Modification

Any modification to this Agreement must be in writing, signed by both parties, and approved by the SSA DIB.

C. Termination

The parties may terminate this Agreement at any time upon mutual written consent of both parties. Either party may unilaterally terminate this Agreement upon 90 days advance written notice to the other party; such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow or terminate this Agreement if SSA determines, in its sole discretion, that the State Agency has violated or failed to comply with this Agreement.

XII. Reimbursement

In accordance with section 1106(b) of the Act, the Commissioner of SSA has determined not to charge the State Agency the costs of furnishing the electronic data from the SSA SORs under this Agreement.

XIII. Disclaimer

SSA is not liable for any damages or loss resulting from errors in the data provided to the State Agency under any IEAs governed by this Agreement. Furthermore, SSA

is not liable for any damages or loss resulting from the destruction of any materials or data provided by the State Agency.

The performance or delivery by SSA of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with proper performance of the official duties and obligations of SSA and the relative importance of this request to others. If for any reason SSA delays or fails to provide services, or discontinues the services or any part thereof, SSA is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

XIV. Points of Contact

A. SSA Point of Contact

San Francisco Regional Office:
Jamie Lucero, Director
San Francisco Regional Office, Center for Disability and Programs Support
1221 Nevin Ave., 6th Floor
Richmond, CA 94801
Phone: 510-970-8297
Fax: 510-970-8101
Email: Jamie.Lucero@ssa.gov

B. State Agency Point of Contact

Sonia Herrera
California Health and Human Services Agency
1600 Ninth Street
Sacramento, CA 95814
Phone: 916-654-3459 / Fax: 916-440-5001
Email: Sonia.Herrera@chhs.ca.gov

XV. SSA and Data Integrity Board Approval of Model CMPPA Agreement

The signatories below warrant and represent that they have the competent authority on behalf of SSA to approve the model of this CMPPA Agreement.

SOCIAL SECURITY ADMINISTRATION

Mary Ann Zimmerman

Mary Ann Zimmerman
Acting Deputy Executive Director
Office of Privacy and Disclosure
Office of the General Counsel

December 21, 2016

Date

I certify that the SSA Data Integrity Board approved the model of this CMPPA Agreement.

Glenn Sklar
Acting Chair
SSA Data Integrity Board

1/30/17

Date

XVI. Authorized Signatures

The signatories below warrant and represent that they have the competent authority on behalf of their respective agency to enter into the obligations set forth in this Agreement.

SOCIAL SECURITY ADMINISTRATION

Grace M. Kim
Regional Commissioner
San Francisco

6/2/17
Date

HEALTH AND HUMAN SERVICES AGENCY

Diana S. Dooley
Secretary

May 24, 2017
Date

ATTACHMENT 2

AUTHORIZED DATA EXCHANGE SYSTEM(S)

Attachment 2

Authorized Data Exchange System(s)

BEER (Beneficiary Earnings Exchange Record): Employer data for the last calendar year.

BENDEX (Beneficiary and Earnings Data Exchange): Primary source for Title II eligibility, benefit and demographic data.

LIS (Low-Income Subsidy): Data from the Low-Income Subsidy Application for Medicare Part D beneficiaries -- used for Medicare Savings Programs (MSP).

Medicare 1144 (Outreach): Lists of individuals on SSA roles, who may be eligible for medical assistance for: payment of the cost of Medicare cost-sharing under the Medicaid program pursuant to Sections 1902(a)(10)(E) and 1933 of the Act; transitional assistance under Section 1860D-31(f) of the Act; or premiums and cost-sharing subsidies for low-income individuals under Section 1860D-14 of the Act.

PUPS (Prisoner Update Processing System): Confinement data received from over 2000 state and local institutions (such as jails, prisons, or other penal institutions or correctional facilities) -- PUPS matches the received data with the MBR and SSR benefit data and generates alerts for review/action.

QUARTERS OF COVERAGE (QC): Quarters of Coverage data as assigned and described under Title II of the Act -- The term "quarters of coverage" is also referred to as "credits" or "Social Security credits" in various SSA public information documents, as well as to refer to "qualifying quarters" to determine entitlement to receive Food Stamps.

SDX (SSI State Data Exchange): Primary source of Title XVI eligibility, benefit and demographic data as well as data for Title VIII Special Veterans Benefits (SVB).

SOLQ/SOLQ-I (State On-line Query/State On-line Query-Internet): A real-time online system that provides SSN verification and MBR and SSR benefit data similar to data provided through SVES.

Attachment 2

SVES (State Verification and Exchange System): A batch system that provides SSN verification, MBR benefit information, and SSR information through a uniform data response based on authorized user-initiated queries. The SVES types are divided into five different responses as follows:

SVES I:	This batch provides strictly SSN verification.
SVES I/Citizenship*	This batch provides strictly SSN verification and citizenship data.
SVES II:	This batch provides strictly SSN verification and MBR benefit information
SVES III:	This batch provides strictly SSN verification and SSR/SVB.
SVES IV:	This batch provides SSN verification, MBR benefit information, and SSR/SVB information, which represents all available SVES data.

** Citizenship status data disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3 is only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants.*

ATTACHMENT 3

SYSTEM SECURITY REQUIREMENTS THROUGH THE ICON SYSTEM

Not Applicable

Attachment 3

Systems Security Requirements for SWA Access to SSA Information Through the ICON System

12/9/2016

Systems Security Requirements for SWA Access to SSA Information Through the ICON System

A. General Systems Security Standards

SWA's that request and receive information from SSA through the ICON system must comply with the following general systems security standards concerning access to and control of SSA information. The SWA must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information retrieved from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The SWA must employ both physical and electronic safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and State laws. SSA may, at its discretion, make on-site inspections or other provisions to ensure that adequate safeguards are being maintained by the SWA.

B. System Security Requirements for SWA's

SWA's that receive SSA information through the ICON system must comply with the following systems security requirements which must be met before DOL will approve a request from an SWA for online access to SSA information through the ICON system. The SWA system security design and procedures must conform to these requirements. They must be documented by the SWA and subsequently certified by either DOL or by an Independent Verification and Validation (IV&V) contractor prior to initiating transactions to and from SSA through the ICON.

No specific format for submitting this documentation to DOL is required. However, regardless of how it is presented, the information should be submitted to DOL in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the SWA. Written documentation should address each of the following security control areas:

1. General System Security Design and Operating Environment

The SWA must provide a written description of its' system configuration and security features. This should include the following:

a. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and

b. A description of how SSA information will be obtained by and presented to SWA users, including sample computer screen presentation formats and an explanation of whether the SWA system will request information from SSA by means of systems generated or user initiated transactions; and

c. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the SWA system and an explanation of their job descriptions.

Meeting this Requirement

SWA's must explain in their documentation the overall design and security features of their system. During onsite certification, the IV&V contractor, or other certifier, will use the SWA's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and for verifying that the SWA systems and procedures conform to SSA requirements.

Following submission to the DOL in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

2. Automated Audit Trail

SWA's receiving SSA information through the ICON system must implement and maintain a fully automated audit trail system capable of data collection, data retrieval and data storage. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator and relevant business purpose (i.e. the SWA client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored

in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before DOL will approve the SWA's request for access to SSA information through the ICON system.

If SSA-supplied information is retained in the SWA system, or if certain data elements within the SWA system will indicate to users that the information has been verified by SSA, the SWA system also must capture an audit trail record of any user who views SSA information stored within the SWA system. The audit trail requirements for these inquiry transactions are the same as those outlined above for SWA transactions requesting information directly from SSA.

Meeting this Requirement

The SWA must include in their documentation a description of their audit trail capability and a discussion of how it conforms to SSA's requirements. During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the system's audit trail and retrieval capability. The SWA must be able to identify employee's who initiate online requests for SSA information (or, for systems generated transaction designs, the SWA case that triggered the transaction), the time and date of the request, and the purpose for which the transaction was originated. The certifier, or IV&V contractor, also will request a demonstration of the system's audit trail capability for tracking the activity of SWA employees that are permitted to view SSA supplied information within the SWA system, if applicable.

During its future compliance reviews (see below), the SSA also will test the SWA audit trail capability by requesting verification of a sample of transactions it has processed from the SWA after implementation of access to SSA information through the ICON system.

3. System Access Control

The SWA must utilize and maintain technological (logical) access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The SWA must use a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. The SWA must have

management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the SWA system.

Meeting this Requirement

The SWA must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the function responsible for PIN/password issuance and maintenance.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions to verify their responsibilities in the SWA's access control process and will observe a demonstration of the procedures for logging onto the SWA system and for accessing SSA information.

4. Monitoring and Anomaly Detection

The SWA's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to an SWA client case (e.g. celebrities, SWA employees, relatives, etc.) If the SWA system design is transaction driven (i.e. employees cannot initiate transactions themselves, rather, the SWA system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an SWA employee unless the SWA system contains a record containing the client's Social Security Number), then the SWA needs only minimal additional monitoring and anomaly detection. If such designs are used, the SWA only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the SWA system by employees not authorized to have access to such information.

If the SWA design does not include either of the security control features described above, then the SWA must develop and implement compensating security controls to prevent their employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of queries requested by individual SWA employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The SWA system must produce reports providing SWA management and/or supervisors with the capability to appropriately monitor user activity, such as:

- User ID exception reports

This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password.

- Inquiry match exception reports

This type of report captures information about users who may be initiating transactions for Social Security Numbers that have no client case association within the SWA system.

- System error exception reports

This type of report captures information about users who may not understand or be following proper procedures for access to SSA information through the ICON system.

- Inquiry activity statistical reports

This type of report captures information about transaction usage patterns among authorized users, which would provide SWA management a tool for monitoring typical usage patterns compared to extraordinary usage.

The SWA must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors, or to local security officers, to ensure that the reports are used by those whose responsibilities include monitoring the work of the authorized users.

Meeting this Requirement

The SWA must explain in their documentation how their system design will monitor and/or prevent their employees from browsing SSA information. If the design is based on a "permission module" (see above), a similar design, or is transaction driven (i.e. no employee initiated transactions) then the SWA does not need to implement additional systematic and/or managerial oversight procedures to monitor their employees access to SSA information. The SWA only needs to monitor user access control violations. The documentation should clearly explain how the system design will prevent SWA employees from browsing SSA records.

If the SWA system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an SWA client), then the SWA must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA

information. The SWA should include sample report formats demonstrating their capability to produce the types of reports described above, and the SWA should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the SWA's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the SWA will demonstrate how the system triggers requests for information from SSA.

- If the design is based on a permission module, the SWA will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the SWA system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the SWA system.)

- If the design is based on systematic and/or managerial monitoring and oversight, the SWA will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification, the IV&V contractor, or other certifier, also will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

5. **Management Oversight and Quality Assurance**

The SWA must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information through the ICON system, and to ensure there is ongoing compliance with the terms of the SWA's data exchange agreement with SSA. The management oversight function must consist of one or more SWA management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to

determine whether the requests comply with these guidelines. These functions should be performed by SWA employees whose job functions are separate from those who request or use information from SSA.

Meeting this Requirement

The SWA must document that they will establish and/or maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information, and oversight and monitoring of the use of SSA information within the SWA business process. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

6. Security Awareness and Employee Sanctions

The SWA must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other Federal and State laws governing use and misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

Meeting this Requirement

The SWA must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The SWA should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The IV&V contractor, or other certifier, also will meet with a sample of SWA employees to assess their level of training and

understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

7. Data and Communications Security

The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

D. Onsite Systems Security Certification Review

The SWA must obtain and participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the ICON system. DOL will require an initial onsite systems security certification review to be performed by either an independent IV&V contractor, or other DOL approved certifier. The onsite certification will address each of the requirements described above and will include, where appropriate, a demonstration of the SWA's implementation of each requirement. The review will include a walkthrough of the SWA's data center to observe and document physical security safeguards, a demonstration of the SWA's implementation of online access to SSA information through the ICON system, and discussions with managers/supervisors. The IV&V contractor, or other certifier, also will visit at least one of the SWA's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.

The IV&V contractor, or other certifier, will separately document and certify SWA compliance with each SSA security requirement. To fully comply with SSA's security requirements and be certified to connect to SSA through the ICON system, the SWA must submit to DOL a complete package of documentation as described above and a complete certification from an independent IV&V contractor, or other DOL approved certifier, that the SWA system design and infrastructure is in agreement with the SWA documentation and consistent with SSA requirements. Any unresolved or unimplemented security control features must be resolved by the SWA before DOL will authorize their connection to SSA through the ICON system.

Following initial certification and authorization from DOL to connect to SSA through the ICON system, SSA is responsible for future systems security compliance reviews. SSA conducts such reviews approximately once every three years, or as needed if there is a significant change in the SWA's computing platform, or if there is a violation of any of SSA's systems security requirements or an unauthorized disclosure of SSA information by the SWA. The format of those reviews generally consists of

reviewing and updating the SWA compliance with the systems security requirements described above.

SENSITIVE DOCUMENT

ATTACHMENT 4

ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES

(Technical Systems Security Requirements- TSSR)

Attachment 4 is a sensitive document, not a public document, and shall not in any manner be made available to the public without prior approval from DHCS.

ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES FOR STATE AND LOCAL AGENCIES EXCHANGING ELECTRONIC INFORMATION WITH THE SOCIAL SECURITY ADMINISTRATION

SENSITIVE DOCUMENT

Version 7.0
July 2015

TABLE OF CONTENTS

1. Introduction

Federal standards require the Social Security Administration (SSA) to maintain oversight of the information it provides to its ***Electronic Information Exchange Partners (EIEPs)***. EIEPs must protect the information with efficient and effective security controls. EIEPs are entities that have electronic information exchange agreements with the agency.

This document consistently references the concept of **Electronic Information Exchange Partners (EIEP)**; however, our **Compliance Review Questionnaire (CRQ)** and **Security Design Plan (SDP)** documents will use the terms "**state agency**" or "**state agency, contractor(s), and agent(s)**" for clarity. Most state officials and agreement signatories are not familiar with the acronym EIEP; therefore, SSA will continue to use the terms "state agency" or "state agency, contractor(s), and agent(s)" in the same manner as the Computer Matching and Privacy Protection Act (CMPPA) and Information Exchange Agreements (IEA). This allows for easier alignment and mapping back to our data exchange agreements between state agencies and SSA. It will also provide a more "user-friendly" experience for the state officials who complete these forms on behalf of their state agencies.

The objective of this document is twofold. The first is to ensure that SSA can properly certify EIEPs as compliant with SSA security standards, requirements, and procedures. The second is to ensure that EIEPs adequately safeguard electronic information provided to them by SSA.

This document helps EIEPs understand the criteria that SSA uses when evaluating and certifying the system design and security features used for electronic access to SSA-provided information. Finally, this document provides the framework and general procedures for SSA's Security Certification and Compliance Review Programs.

The primary statutory authority that supports the information contained in this document is the **Federal Information Security Management Act (FISMA)**. FISMA became law as part of the **Electronic Government Act of 2002.** FISMA is the United States legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or manufactured threats. FISMA assigned the **National Institute of Standards and Technology (NIST)**, a branch of the U.S. Department of Commerce, the responsibility to outline and define compliance with FISMA. Unless otherwise stated, all of SSA's requirements mirror the NIST-defined management, operational, and technical controls listed in the various NIST Special Publications (SP) libraries of technical guidance documents.

To gain electronic access to SSA-provided information, under the auspices of a data exchange agreement, EIEP's must comply with SSA's most current **Technical System Security Requirements** (hereafter referred to as **TSSRs)** to gain access to SSA-provided information. This document is synonymous with the **Electronic Information Exchange Security Requirements and Procedures for State and**

Local Agencies Exchanging Electronic Information with the Social Security Administration in the agreements. The TSSR specifies minimally acceptable levels of security standards and controls to protect SSA-provided information. SSA maintains the TSSR as a living document—subject to change--that addresses emerging threats, new attack methods and the development of new technology that potentially places SSA-provided information at risk. EIEPs may proactively ensure their ongoing compliance to the TSSR by periodically requesting the most current version from SSA. SSA will work with EIEPs to resolve deficiencies, which result from updates to the TSSRs. SSA refers to this process as **Gap Analysis**. EIEPs may proactively ensure their ongoing compliance with the TSSRs by periodically requesting the most current TSSR package from their SSA Point of Contact (POC) from the data exchange agreement.

SSA's standard for categorization of information (Moderate) and information systems is to provide appropriate levels of security according to risk level. Additions, deletions, or modification of security controls directly affect the level of security and due diligence SSA requires EIEPs use to mitigate risks. The emergence of new threats, attack methods, and the development of new technology warrants frequent reviews and revisions to our TSSR. Consequently, EIEPs should expect SSA's TSSR to evolve in harmony with the industry.

2. Electronic Information Exchange (EIE) Definition

For discussion purposes herein, EIE is any electronic process in which SSA discloses information under its control to any third party for program or non-program purposes, without the specific consent of the subject individual or any agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the programmatic systems of parties to electronic information sharing agreements with SSA. This includes direct terminal access (DTA) to SSA systems, batch processing, and variations thereof (e.g., online query) regardless of the systematic method used to accomplish the activity or to interconnect SSA with the EIEP.

3. Roles and Responsibilities

The SSA ***Office of Information Security (OIS)*** has agency-wide responsibility for interpreting, developing, and implementing security policy; providing security and integrity review requirements for all major SSA systems; managing SSA's fraud monitoring and reporting activities, developing and disseminating security training and awareness materials, and providing consultation and support for a variety of agency initiatives. SSA's security reviews ensure that external systems receiving information from SSA are secure and operate in a manner consistent with SSA's Information Technology (IT) security policies and in compliance with the terms of electronic data exchange agreements executed by SSA with outside entities. Within the context of SSA's security policies and the terms of the electronic data exchange

agreements with SSA's EIEPs, SSA exclusively conducts and brings to closure initial security certifications and triennial security compliance reviews. This includes (but not limited to) any EIEP that processes, maintains, transmits, or stores SSA-provided information in accordance with pertinent Federal requirements.

a. The SSA Regional ***Data Exchange Coordinators*** (DECs) serve as a bridge between SSA and EIEPs. DECs assist in coordinating data exchange security review activities with EIEPs; (e.g., providing points of contact with state agencies, assisting in setting up security reviews, etc.) DECs are also the first points of contact for states if an employee of a state agency or an employee of a state agency's contractor or agent becomes aware of suspected or actual loss of SSA-provided information.

b. SSA requires **EIEPs** to adhere to the standards, requirements, and procedures, published in this TSSR document.

   - "Personally Identifiable Information (PII)," covered under several Federal laws and statutes, refers to specific information about an individual used to trace that individual's identity. Information such as his/her name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records, alone, or when combined with other personal or identifying information is linkable or lined to a specific individual's medical, educational, financial, and employment information.

   - The data (last 4 digits of the SSN) that SSA provides to its EIEPs for purposes of the Help America Vote Act (HAVA) does not identify a specific individual; therefore, is not "PII" as defined by the Act.

   - Both SSA and EIEPs must remain diligent in the responsibility for establishing ***appropriate*** management, operational, and technical safeguards to ensure the confidentiality, integrity, and availability of its records and to protect against any anticipated threats or hazards to their security or integrity.

c. A State Transmission/Transfer Component (STC) is an organization that performs as an electronic information conduit or collection point for one of more other entities (also referred to as a hub). An STC must also adhere to the same management, operational and technical controls as SSA and the EIEP.

NOTE: Disclosure of Federal Tax Information (FTI) is limited to certain Federal agencies and state programs supported by federal statutes under Sections 1137, 453, and 1106 of the Social Security Act. For information regarding

***safeguards for protecting FTI, consult IRS Publication 1075,* Tax Information Security Guidelines for Federal, State, and Local Agencies.**

4. General Systems Security Standards

EIEPs that request and receive information electronically from SSA must comply with the following general systems security standards concerning access to and control of SSA-provided information.

NOTE: EIEPs may not create separate files or records comprised solely of the information provided by SSA.

1. EIEPs must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA-provided information neither prevents nor impedes the EIEP's ability to:

    - safeguard the information in conformance with SSA requirements
    - efficiently investigate fraud, data breaches, or security events that involve SSA-provided information
    - detect instances of misuse or abuse of SSA-provided information

For example, Utilization of cloud computing may have the potential to jeopardize an EIEP's compliance with the terms of their agreement or associated systems security requirements and procedures.

2. The EIEP must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.
3. The EIEP must use the software and/or devices provided to the EIEPs only in support of the current agreement(s) between the EIEPs and SSA.
4. SSA prohibits the EIEP from modifying any software or devices provided to the EIEPs by SSA.
5. EIEPs must ensure that SSA-provided information is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in geographic or virtual areas not subject to U.S. law.
6. EIEPs must restrict access to the information to authorized users who need it to perform their official duties.

    NOTE: Contractors and agents (hereafter referred to as contractors) of the EIEP who process, maintain, transmit, or store SSA-provided information are held to the same security requirements as employees of the EIEP. Refer to the section 'Contractors of Electronic Information Exchange Partners in the Systems Security Requirements for additional information.

7. EIEPs must store information received from SSA in a manner that, at all times, is

physically and electronically secure from access by unauthorized persons.

8. The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel.

9. EIEPs must employ both physical and technological barriers to prevent unauthorized retrieval of SSA-provided information via computer, remote terminal, or other means.

10. EIEPs must have formal PII incident response procedures. When faced with a security incident, caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA-provided information affected by the incident.

11. EIEPs must have an active and robust security awareness program, which is mandatory for all employees who access SSA-provided information.

12. EIEPs must advise employees with access to SSA-provided information of the confidential nature of the information, the safeguards required to protecting the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and state laws.

13. In accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) on Contingency Planning requirements and recommendations, SSA requires EIEPs to document a senior management approved Contingency plan that includes a disaster recovery plan that addresses both natural disaster and cyber-attack situations.

14. SSA requires the Contingency Plan to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that address the security of SSA-provided information if a disaster occurs.

15. At its discretion, SSA or its designee must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5. Systems Security Requirements

5.1 Overview

SSA's TSSR represent the current industry standard for security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations, statutes, standards, and guidelines. Additionally, SSA's TSSR includes organizationally defined interpretations, policies, and procedures mandated by the authority of the Commissioner of Social Security in areas when or where other cited authorities may be silent or non-specific.

SSA must certify that the EIEP has implemented security controls that meet the requirements and work as intended, before the authorization to initiate transactions to and from SSA, through batch data exchange processes or online processes such as State Online Query (SOLQ) or Internet SOLQ (SOLQ-I).

The TSSR address management, operational, and technical controls regarding security safeguards to ensure only authorized disclosure and usage of SSA provided information used, maintained, transmitted, or stored by SSA's EIEPs. SSA requires EIEPs to maintain an organizational access control structure that adheres to a three-tiered best practices model. The SSA recommended model is "separation of duties," "need-to-know" and "least privilege."

SSA requires EIEPs to document and notify SSA prior to sharing SSA-provided information with another state entity, or to allow them direct access to their system. **This includes (but not limited to) law enforcement, other state agencies, and state organizations that perform audit, quality, or integrity functions.**

SSA recommends that the EIEP develop and publish a comprehensive Information Technology (IT) Systems Security Policy document that specifically addresses:

1) the classification of information processed and stored within the network,

2) management, operational, and technical controls to protect the information stored and processed within the network,

3) access to the various systems and subsystems within the network,

4) Security Awareness Training,

5) Employee and End User Sanctions Policy,
6) Contingency Planning and Disaster Recovery

7) Incident Response Policy, and

8) The disposal of protected information and sensitive documents derived from the system or subsystems on the network.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.2 General System Security Design and Operating Environment *(Planning (PL) Family – (System Security Plan), Contingency Plan (CP) Family, Physical and Environmental (PE) Family, NIST SP 800-53 rev. 4)*

In accordance with the NIST suite of Special Publications (SP) (e.g., 800-53, 800-34, etc.), SSA requires the EIEP to maintain policies, procedures, descriptions, and explanations of their overall system design, configuration, security features, and operational environment. They should include explanations of how they conform to SSA's TSSRs. The EIEPs General System Security design and Operating Environment must also address:

a) the operating environment(s) in which the EIEP will utilize, maintain, store, and transmit SSA-provided information,

b) the business process(es) in which the EIEP will use SSA-provided information,

c) the physical safeguards employed to ensure that unauthorized personnel, the public or visitors to the agency cannot access SSA-provided information,

d) details of how the EIEP keeps audit information pertaining to the use and access to SSA-provided information and associated applications readily available,

e) electronic safeguards, methods, and procedures for protecting the EIEP's network infrastructure and for protecting SSA-provided information while in transit, in use within a process or application, and at rest ,

f) a senior management approved Information System Contingency Plan (ISCP) that addresses both internal and external threats. SSA requires the ISCP to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that addresses the security of SSA-provided information if a disaster occurs. SSA recommends that state agencies perform disaster exercises at least once annually.,

g) how the EIEP prevents unauthorized retrieval of SSA-provided information by computer, remote terminal, or other means; including descriptions of security software other than access control software (e.g., security patch and anti-malware software installation and maintenance, etc.)

h) how the configurations of devices (e.g., servers, workstations, portable devices) involving SSA-provided information complies with recognized industry standards (i.e. NIST SP's) and SSA's TSSR, and

i) organizational structure of the agency, number of users, and all external entities that will have access to the system and/or application that displays, transmits, and/or application that displays, transmits and/or stores SSA-provided information.

Note: At its discretion, SSA or a third party (i.e. contractor) must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.3 System Access Control
(Access Control (AC) Family, NIST SP 800-53 rev. 4)

EIEPs must utilize and maintain technological (logical) access controls that limit access to SSA-provided information and associated transactions and functions to only those users, processes acting on behalf of authorized users, or devices (including other information systems) authorized for such access based on their official duties or purpose(s). EIEPs must employ a recognized user-access security software package (e.g.,RAC-F, ACF-2, TOP SECRET, Active Directory, etc.) or a security software design, which is equivalent to such products. The access control software must employ and enforce (1) PIN/password, and/or (2) PIN/biometric identifier, and/or (3) SmartCard/biometric identifier, etc., (for authenticating users), (and lower case letters, numbers, and special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

The EIEP's password policies must require stringent password construction as supported by current NIST guidelines for the user accounts of persons, processes, or devices whose functions require access privileges above those of ordinary users. **SSA strongly recommends Two-Factor Authentication.**

The EIEP's implementation of the control software must comply with recognized industry standards. Password policies should enforce sufficient construction strength (length and complexity) to defeat or minimize risk-based identified vulnerabilities and ensure limitations for password repetition. Technical controls should enforce periodic password changes based on a risk-based standard (e.g., maximum password age of 90 days, minimum password age of 3 – 7 days) and enforce automatic disabling of user accounts that have been inactive for a specified period of time (e.g., 90 days).

The EIEP's password policies must require stringent password construction (e.g., passwords greater than eight characters in length requiring upper and lower case letters, numbers, and/or special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

In addition, SSA has the following specific requirements in the area of Access Control:

1. Upon hiring or before granting access to SSA-provided information, EIEPs should verify the identities of any employees, contractors, and agents who will have access to SSA-provided information in accordance with the applicable agency or state's "personnel identity verification policy."

2. SSA requires that state agencies have a logical control feature that designates a maximum number of unsuccessful login attempts for agency workstations and devices that store or process SSA-provided information, in accordance with NIST guidelines. SSA recommends no fewer than three (3) and no greater than five (5)..

3. SSA requires that the state agency designate specific official(s) or functional component(s) to issue PINs, passwords, biometric identifiers, or Personal Identity Verification (PIV) credentials to individuals who will access SSA-provided information. **SSA also requires that the state agency prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job-function or category of access.**

4. SSA requires that EIEPs grant access to SSA-provided information based on least privilege, need-to-know, and separation of duties. State agencies should not routinely grant employees, contractors, or agents access privileges that exceed the organization's business needs. SSA also requires that EIEPs periodically review employees, contractors, and agent's system access to determine if the same levels and types of access remain applicable.

5. If an EIEP employee, contractor, or agent is subject to an adverse administrative action by the EIEP (e.g., reduction in pay, disciplinary action, termination of employment), SSA recommends the EIEP remove his or her access to SSA-provided information in advance of the adverse action to reduce the possibility that will the employee will perform unauthorized activities that involve SSA-provided information.

6. SSA requires that work-at-home, remote access, and/or Internet access comply with applicable Federal and state security policy and standards. Furthermore, the EIEPs access control policy must define the safeguards in place to adequately protect SSA-provided information for work-at-home, remote access, and/or Internet access.

7. SSA requires EIEPs to design their system with logical control(s) that prevent unauthorized browsing of SSA-provided information. SSA refers to this setup as a **Permission Module.** The term "**Permission Module**" supports a business rule and systematic control that prevents users from browsing a system that contains SSA-provided information. It also supports the principle of **referential integrity**. It should prevent non-business related or unofficial access to SSA-provided information. Before a user or process requests SSA-provided information for verification, the system should verify it is an authorized transaction. Some organizations use the term "referential integrity" to describe the verification step. A properly configured Permission Module should prevent a user from performing any actions not consistent with a need-to-know business process. If a logical permission module configuration is not possible, the state agency must enforce its Access Control List (ACL) in accordance with the principle of least privilege. **The only acceptable compensating control for a system that lacks a permission module is a 100% review of all transactions that involve SSA-provided information.**

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.4 Automated Audit Trail

(Audit and Accountability (AU) Family, NIST SP 800-53 rev. 4)

SSA requires EIEPs, and other STCs or agencies that provide audit trail services to other state agencies that receive information electronically from SSA, to implement and maintain a fully automated audit trail system (ATS). The system must be capable of creating, storing, protecting, and (efficiently) retrieving and collecting records identifying the individual user who initiates a request for information from SSA or accesses SSA-provided information. At a minimum, individual audit trail records must contain the data needed (including date and time stamps) to associate each query transaction or access to SSA-provided information with its initiator, their action, if any, and the relevant business purpose/process (e.g., SSN verification for Medicaid). Each entry in the audit file must be stored as a separate record, not overlaid by subsequent records. The ATS must create transaction files to capture all input from interactive internet applications that access or query SSA-provided information.

SSA requires that the agency's ATS create an audit record when users view screens that contain SSA-provided information. If an STC handles and audits the EIEP's transactions with SSA, the EIEP is responsible for ensuring that the STC's audit capabilities meet NIST's guidelines for an automated audit trail system. The EIEP must also establish a process to obtain specific audit information from the STC regarding the EIEP's SSA transactions.

SSA requires that EIEPs have automated retrieval and collection of audit records. Such automated functions can be via online queries, automated reports, batch processing, or any other logical means of delivering audit records in an expeditious manner. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request.

Access to the audit file must be restricted to authorized users with a "need to know," audit file data must be unalterable (read-only), and maintained for a minimum of three (3) (preferably seven (7)) years. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request. The EIEP must backup audit trail records on a regular basis to ensure its availability. EIEPs must apply the same level of protection to backup audit files that apply to the original files to ensure the integrity of the data.

If the EIEP retains SSA-provided information in a database (e.g., Access database, SharePoint, etc.), or if certain data elements within the EIEP's system indicates to users that SSA verified the information, the EIEP's system must also capture an audit trail record of users who view SSA-provided information stored within the EIEP's system. The retrieval requirements for SSA-provided information at rest and the retrieval requirements for regular transactions are identical. **Similar to the Permission Module requirement above, the only acceptable compensating control for a system that lacks an Automated Audit Trail System (ATS) is a 100% review of all transactions that involve SSA-provided information.**

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.5 Personally Identifiable Information (PII)

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and AP Family – Authority and Purpose (Privacy Controls), NIST SP 800-53 rev. 4)

Personally Identifiable Information (PII) is information used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, alone or when combined with other personal or identifying information linked or linkable to a specific individual. An item such as date and place of birth, mother's maiden name, or father's surname is PII, regardless of whether combined with other data.

SSA defines ***a PII loss*** as a circumstance when an EIEP employee, contractor, or agent has reason to believe that information on hard copy or in electronic format, which contains PII provided by SSA, left the EIEP's custody or the EIEP disclosed it to an unauthorized individual or entity. PII loss is a reportable incident. SSA requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain SSA-provided information.

If a PII loss involving SSA-provided information occurs or is suspected, the EIEP must be able to quantify the extent of the loss and compile a complete list of the individuals potentially affected by the incident (refer to ***Incident Reporting***).

The EIEP should have procedural documents to describe methods and controls for safeguarding SSA-provided PII while in use, at rest, during transmission, or after archiving. The document should explain how the EIEP manages and handles SSA-provided information on print media and explain how the methods and controls conform to NIST requirements. SSA requires that printed items that contain SSA-provided PII always remain in the custody of authorized EIEP employees, contractors, or agents. SSA also requires that the agency destroy the items when no longer required for the EIEP's business process. If retained in paper files for evidentiary purposes, the EIEP should safeguard such PII in a manner that prevents unauthorized personnel from accessing such materials. All agencies that receive SSA-provided information must maintain an inventory of all documents that outline statewide or agency policy and procedures regarding the same.

5.6 Monitoring and Anomaly Detection

(Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-137, E-Government Act of 2002 (P.L. 107-347), and Security Assessment and Authorization (CA) and Risk Assessment (RA) Families, NIST SP 800-53 rev. 4)

SSA requires that the EIEPs use an Intrusion Protection System (IPS) or an Intrusion Detection System (IDS). The EIEP must establish and/or maintain continuous monitoring of its network infrastructure and assets to ensure that:

1) the EIEP's security controls continue to be effective over time,

2) the EIEP uses industry-standard Security Information Event Manager (SIEM) tools, anti-malware software, and effective antivirus protection,

3) only authorized individuals, devices, and processes have access to SSA-provided information,

4) the EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions (e.g., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) as soon as they occur,

5) the necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes,

6) upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk,

7) in the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions, and

8) trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are readily discernible.

The EIEP's system must include the capability to prevent users from unauthorized browsing of SSA records. SSA requires the use of a transaction-driven **permission module design**, whereby employees are unable to initiate transactions not associated with the normal business process. If the EIEP uses such a design, they also must have anomaly detection to monitor an employee's unauthorized attempts to gain access to SSA-provided information and attempts to obtain information from SSA for clients not in the EIEP's client system. The EIEP should employ measures to ensure the permission module's integrity. Users should not be able to create a bogus case and subsequently delete it in such a manner that it goes undetected. The SSA permission module design employs both role and rules based logical access control restrictions. (Refer to ***Access Control***)

If the EIEP's design ***does not use*** a permission module ***and*** is not transaction-driven, until at least one of these security features exists, the EIEP must develop and implement **compensating security controls** to deter employees from browsing SSA records. These controls must include monitoring and anomaly detection features, such as: systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of transactions or queries requested or initiated by individuals and include systematic or manual procedures for verifying that requests and queries of SSA-provided information comply with valid official business purposes.

Risk Management Program

SSA recommends that EIEPs develop and maintain a published Risk Assessment Policy and Procedures document. A Risk Management Program may include, but is not limited to the following:

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance,

2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls,

3. A function that conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits,

4. An independent function that conducts vulnerability and risk assessments, reviews risk assessment results, and disseminates such information to senior management,

5. A firm commitment from senior management to update the risk assessment whenever there are significant changes to the information

system or environment of operation or other conditions that may affect the security of SSA-provided information,

6. A robust vulnerability scanning protocol that employs industry standard scanning tools and techniques that facilitate interoperability among tools and automates parts of the vulnerability management process,

7. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk, and

8. Shares information obtained from the vulnerability scanning process and security control assessments with senior management to help eliminate similar vulnerabilities in other information systems that receive, process, transmit, or store SSA-provided information.

Note: The EIEP's decision to initiate or maintain an official Risk Management Program and establish a formal Risk Assessment Strategy for mitigating risk is strictly voluntary, but highly recommended by SSA.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.7 Management Oversight and Quality Assurance

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the AC – Access Control & PM – Program Management Families, NIST SP 800-53 rev. 4)

SSA requires the EIEP to establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized users have access to SSA-provided information. This will ensure there is ongoing compliance with the terms of the EIEP's electronic information sharing agreement with SSA and the TSSRs established for access to SSA-provided information. The entity responsible for management oversight should consist of one or more of the EIEP's management officials whose job functions include responsibility to ensure that the EIEP only grants access to the appropriate users and position types (least privilege), which require the SSA-provided information to do their jobs (need-to-know).

SSA requires the EIEP to ensure that users granted access to SSA-provided information receive adequate training on the sensitivity of the information, associated safeguards, operating procedures, and the civil and criminal consequences or penalties for misuse or improper disclosure.

SSA requires that EIEPs establish the following job functions and require that only users whose job functions are separate from personnel who request or use SSA-provided information.

SSA requires that EIEPs establish the following job functions separate from personnel who request or use SSA-provided information.

a) Perform periodic self-reviews to monitor the EIEP's ongoing usage of SSA-provided information.

b) Perform random sampling of work activity that involves SSA-provided information to determine if the access and usage comply with SSA's requirements

SSA requires the EIEP's system to produce reports that allow management and/or supervisors to monitor user activity. The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

1. **User ID Exception Reports:**

   This type of report captures information about users who enter incorrect user IDs when attempting to gain access to the system or to a transaction that initiates requests for information from SSA, including failed attempts to enter a password.

2. **Inquiry Match Exception Reports:**

   This type of report captures information about users who initiate transactions for SSNs that have no client case association within the EIEP's system **(the EIEP's management must review 100% of these cases).**

3. **System Error Exception Reports:**

   This type of report captures information about users who may not understand or may be violating proper procedures for access to SSA-provided information.

4. **Inquiry Activity Statistical Reports:**

   This type of report captures information about transaction usage patterns among authorized users and is a tool that enables the EIEP's management to monitor typical usage patterns in contrast to extraordinary usage patterns.

The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.8 Data and Communications Security

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Access Control (AC), Configuration Management (CM), Media Protection (MP), and System and Communication (SC) Families, NIST SP 800-53 rev. 4)

SSA requires EIEPs to encrypt PII and SSA-provided information when transmitting across dedicated communications circuits between its systems, intrastate communications between its local office locations, and on the EIEP's mobile computers, devices and removable media. The EIEP's encryption methods must align with the Guidelines established by the National Institute of Standards and Technology (NIST). SSA recommends the Advanced Encryption Standard (AES) or Triple DES (Data Encryption Standard 3). **Files encrypted for external users (when using tools such as Microsoft Word encryption,) require a key length of at least nine characters.** SSA recommends that the key (also referred to as a password) contain both special characters and numbers. SSA supports the NIST Guidelines that requires the EIEP deliver the key so that it does not accompany the media. The EIEP must secure the key when not in use or unattended.

SSA discourages the use of the public Internet for transmission of SSA-provided information. If, however, the EIEP uses the public Internet or other electronic communications, such as emails and faxes to transmit SSA-provided information, they must use a secure encryption protocol such as Secure Socket Layer (SSL) or Transport Layer Security (TLS). SSA also recommends 256-bit encryption protocols or more secure methods such as Virtual Private Network technology. The EIEP should only send data to a secure address or device to which the EIEP can control and limit access to only specifically authorized individuals and/or processes. **SSA recommends that EIEPs use Media Access Control (MAC) Filtering and Firewalls to protect access points from unauthorized devices attempting to connect to the network.**

EIEPs should not retain SSA-provided information any longer than business purpose(s) dictate. The IEA with SSA stipulates a time for data retention. The EIEP should delete, purge, destroy, or return SSA-provided information when the business purpose for retention no longer exists.

The EIEP may not save or create separate files comprised solely of information provided by SSA. The EIEP may apply specific SSA-provided information to the EIEP's matched record from a preexisting data source. Federal law prohibits duplication and redisclosure of SSA-provided information without written approval from SSA.

This prohibition applies to both internal and external sources who do not have a "need-to-know." SSA recommends that EIEPs use either **Trusted Platform Module (TPM)** or **Hardware Security Module (HSM)** technology solutions to encrypt data at rest on hard drives and other data storage media.

SSA requires EIEPs to prevent unauthorized disclosure of SSA-provided information after they complete processing and after the EIEP no longer requires the information. The EIEP's operational processes must ensure that no residual SSA-provided information remains on the hard drives of user's workstations after the user exits the application(s) that use SSA-provided information. If the EIEP must send a computer, hard drive, or other computing or storage device offsite for repair, the EIEP must have a non-disclosure clause in their contract with the vendor. If the EIEP used the item in connection with a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the EIEP's vendor contract. The EIEP must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the EIEP to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

To sanitize media, the EIEP should use one of the following methods:

1. **Overwriting/Clearing:**

   Overwrite utilities can only be used on working devices. Overwriting is appropriate only for devices designed for multiple reads and writes. The EIEP should overwrite disk drives, magnetic tapes, floppy disks, USB flash drives, and other rewriteable media. The overwrite utility must completely overwrite the media. SSA recommends the use of ***purging*** media sanitization to make the data irretrievable, protecting data against laboratory attacks or forensics. Reformatting the media does not overwrite the data.

2. **Degaussing:**

   Degaussing is a sanitization method for magnetic media (e.g., disk drives, tapes, floppies, etc.). Degaussing is not effective for purging non-magnetic media (e.g., optical discs). SSA and NIST Guidelines require EIEP to use a certified tool designed to degauss each particular type of media. NIST guidelines require certification of the tool to ensure that the magnetic flux applied to the media is strong enough to render the information irretrievable. The degaussing process must render data on the media irretrievable by a laboratory attack or laboratory forensic procedures.

3. **Physical destruction:**

NIST guidelines require physical destruction when degaussing or over-writing cannot be accomplished (for example, CDs, floppies, DVDs, damaged tapes, hard drives, damaged USB flash drives, etc.). Examples of physical destruction include shredding, pulverizing, and burning.

State agencies may retain SSA-provided information in hardcopy only if required to fulfill evidentiary requirements, provided the agencies retire such data in accordance with applicable state laws governing state agency's retention of records. The EIEP must control print media containing SSA-provided information to restrict access to authorized employees who need such access to perform official duties. EIEPs must destroy print media containing SSA-provided information in a secure manner when no longer required for business purposes. SSA requires the EIEP to destroy paper documents that contain SSA-provided information by burning, pulping, shredding, macerating, or other similar means that ensure the information is unrecoverable.

State agencies may use any accretions, deletions, or changes to the SSA-provided information governed by the CMPPA agreement to update their master files or federally funded state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing State Agencies' retention of records.

NOTE: Hand tearing or lining through documents to obscure information does not meet SSA's requirements for appropriate destruction of PII.

The EIEP must employ measures to ensure that communications and data furnished to SSA contain no viruses or other malware.

Special Note regarding Cloud Service Providers:

If the EIEP will store SSA-provided information through a Cloud Service Provider, please provide the name and address of the cloud provider. Describe the security responsibilities the contract requires to protect SSA-provided information.

SSA will ask for detailed descriptions of the security features contractually required of the cloud provider and information regarding how they will protect SSA-provided information at rest and when in transit.

EIEPs cannot legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.9 Incident Reporting

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Incident Response (IR) Family, NIST SP 800-53 rev. 4)

FISMA, NIST Guidelines, and Federal Law require the EIEP to develop and implement policies and procedures to respond to potential data breaches or PII loses. EIEPs must articulate, in writing, how the policies and procedures conform to SSA's requirements. The procedures must include the following information:

> *If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact* ***within one hour****, the responsible State Agency official or delegate must report the incident by contacting* ***SSA's National Network Service Center (NNSC) toll free at 877-697-4889*** *(select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

If SSA, or another Federal investigating entity (e.g. TIGTA or DOJ), determines that the risk presented by a breach or security incident requires that the state agency notify the subject individuals, the agency must agree to absorb all costs associated with notification and remedial actions connected to security breaches. **SSA and NIST Guidelines encourage agencies to consider establishing incident response teams to address PII and SSA-provided information breaches.**

Incident reporting policies and procedures are part of the security awareness program. Incident reporting pertains to all employees, contractors, or agents regardless as to whether they have direct responsibility for contacting SSA. The written policy and procedures document should include specific names, titles, or functions of the individuals responsible for each stage of the notification process. The document should include detailed instructions for how, and to whom each employee, contractor, or agent should report the potential breach or PII loss.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.10 Security Awareness Training and User Sanctions

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)

The EIEP must have an active and robust security awareness program and security training for all employees, contractors, and agents who access SSA-provided information. The training and awareness programs must include:

a. the sensitivity of SSA-provided information and addresses the Privacy Act and other Federal and state laws governing its use and misuse,

b. the rules of behavior concerning use and security in systems and/or applications processing SSA-provided information,

c. the restrictions on viewing and/or copying SSA-provided information,

d. the responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of SSA-provided information,

e. the proper disposal of SSA-provided information,

f. the security breach and data loss incident reporting procedures,

g. the basic understanding of procedures to protect the network from malware attacks,

h. spoofing, phishing and pharming, and network fraud prevention, and

i. the possible criminal and civil sanctions and penalties for misuse of SSA-provided information.

SSA requires the EIEP to provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.

SSA requires the EIEP to provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, or agent who views SSA-provided information also certify that they understand the potential criminal and administrative sanctions or penalties for unlawful disclosure. SSA requires the state agency to require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. The non-disclosure attestation must also include acknowledgement from each employee, contractor, and agent that he or she understands and accepts the potential criminal and/or civil sanctions or penalties associated with misuse or unauthorized disclosure of SSA-provided information. The state agency must retain the non-disclosure attestations for at least five (5) to seven (7) years for each individual who processes, views, or encounters SSA-provided information as part of their duties.

SSA strongly recommends the use of login banners, emails, posters, signs, memoranda, special events, and other promotional materials to encourage security awareness throughout your enterprise.

The state agency must designate a department or party to take the responsibility to provide ongoing security awareness training for all employees, contractors, and agents who access SSA-provided information. Training must include:

- The sensitivity of SSA-provided information and address the Privacy Act and other Federal and state laws governing its use and misuse
- Rules of behavior concerning use and security in systems processing SSA-provided information
- Restrictions on viewing and/or copying SSA-provided information
- The employee, contractor, and agent's responsibility for proper use and protection of SSA-provided information
- Proper disposal of SSA-provided information
- Security incident reporting procedures
- Basic understanding of procedures to protect the network from malware attacks

- Spoofing, Phishing and Pharming scam prevention
- The possible sanctions and penalties for misuse of SSA-provided information

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.11 Contractors of Electronic Information Exchange Partners

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Risk Assessment (RA), System and Services Acquisition (SA), Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)

The state agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by the Agreement may be subject to both civil and criminal sanctions pursuant to applicable Federal statutes. The state agency will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing the Agreement, and thereafter at SSA's request, the state agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

Contractors of the state agency must adhere to the same security requirements as employees of the state agency. The state agency is responsible for the oversight of its contractors and the contractor's compliance with the security requirements. The state agency must enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties. Such contractors or agents agree to abide by all relevant Federal laws, restrictions on access, use, disclosure, and the security requirements contained within the state agency's agreement with SSA.

The state agency must provide proof of the contractual agreement with all contractors and agents who encounter SSA-provided information as part of their duties. If the contractor processes, handles, or transmits information provided to the state agency by SSA or has authority to perform on the state agency's behalf, the state agency should clearly state the specific roles and functions of the contractor within the agreement. The state agency will provide SSA written certification that the contractor is meeting the terms of the agreement, including SSA security requirements. The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to SSA-provided information.

The state agency must also require that contractors and agents who will process, handle, or transmit information provided to the state agency by SSA to include language in their signed agreement that obligates the contractor to follow the terms of the state agency's data exchange agreement with SSA. The state agency must also make certain that the contractor and agent's employees receive the same security awareness training as the state agency's employees. The state agency, the contractor, and the agent should maintain awareness-training records for their employees and require the same mandatory annual

certification procedures.

SSA requires the state agency to subject the contractor to ongoing security compliance reviews that must meet SSA standards. The state agency will conduct compliance reviews at least triennially commencing no later than three (3) years after the approved initial security certification to SSA. The state agencies will provide SSA with documentation of their recurring compliance reviews of their contractors and agents. The state agencies will provide the documentation to SSA during their scheduled compliance and certification reviews or upon SSA's request.

If the state agency's contractor will be involved with the processing, handling, or transmission of information provided to the EIEP by SSA offsite from the EIEP, the EIEP must have the contractual option to perform onsite reviews of that offsite facility to ensure that the following meet SSA's requirements:

a) safeguards for sensitive information,

b) technological safeguards on computer(s) that have access to SSA-provided information,

c) security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and redisclosure of SSA-provided information, and

d) continuous monitoring of the EIEP contractors or agent's network infrastructures and assets.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.12 Cloud Service Providers (CSP) for Electronic Information Exchange Partners

(NIST SP 800-144, NIST SP 800-145, NIST SP 800-146, OMB Memo M-14-03, NIST SP 137)

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 defines Cloud Computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." The three service models, as defined by NIST SP 800-145 are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The Deployment models are Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud. Furthermore, The Federal Risk and Authorization Program (FedRAMP) is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

SSA requires the State Agency, contractor(s), and agent(s) to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

SSA requires the State Agency, contractor(s), and agent(s) to agree that any state-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the State Agency and is subject to onsite inspection and review by the State Agency or SSA with prior notice.

SSA requires that the State Agency thoroughly describe all specific contractual obligations of each party to the Cloud Service Provider (CSP) agreement between the state agency and the CSP vendor(s). If the obligations, services, or conditions widely differ from agency to agency, we require separate SDP Questionnaires to address the CSP services provided to each state agency involved in the receipt, processing, storage, or disposal of SSA-provided information.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6. Security Certification and Compliance Review Programs
(NIST SP 800-18 – System Security Plans and Planning (PL) Family, NIST SP 800-53 rev. 4)

SSA's security certification and compliance review programs are distinct processes. The certification program is a unique episodic process when an EIEP initially requests electronic access to SSA-provided information or makes substantive changes to existing exchange protocol, delivery method, infrastructure, or platform. The certification process entails two stages (refer to 6.1 for details) intended to ensure that management, operational, and technical security measures work as designed. SSA must ensure that the EIEPs fully conform to SSA's security requirements at the time of certification and satisfy both stages of the certification process before SSA will permit online access to its data in a production environment.

The compliance review program entails cyclical security review of the EIEP performed by, or on behalf of SSA. The purpose of the review is to to assess an EIEP's conformance to SSA's current security requirements at the time of the review engagement. The compliance review program applies to both online and batch access to SSA-provided information. Under the compliance review program, EIEPs are subject to ongoing and periodic security reviews by SSA.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.1 The Security Certification Program
(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

The security certification process applies to EIEPs that seek online electronic access to SSA-provide information and consists of two general phases:

a) **Phase 1:** The Security Design Plan (SDP) is a formal written plan authored by the EIEP to document its management, operational, and technical security controls to safeguard SSA-provided information (refer to ***Documenting Security Controls in the Security Design Plan)***.

NOTE: **SSA may have legacy EIEPs (EIEPs not certified under the current process) who have not prepared an SDP. SSA strongly recommends that these EIEPs prepare an SDP.**

The EIEP's preparation and maintenance of a current SDP will aid them in determining potential compliance issues prior to reviews, assuring continued compliance with SSA's TSSRs, and providing for more efficient security reviews.

b) **Phase 2:** The SSA Onsite Certification is a formal security review conducted by SSA, or on its behalf, to examine the full suite of management, operational, and technical security controls implemented by the EIEP to safeguard data obtained from SSA electronically (refer to ***The Certification Process***).

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.2 Documenting Security Controls in the SDP

(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

6.2.1 When an SDP is required:

EIEPs must submit an SDP when one or more of the following circumstances apply:

a) to obtain approval for requested access to SSA-provided information for an initial agreement,

b) to obtain approval to reestablish previously terminated access to SSA-provided information,

c) to obtain approval to implement a new operating or security platform that will involve SSA-provided information,

d) to obtain approval for significant changes to the EIEP's organizational structure, technical processes, operational environment, or security implementations planned or made since approval of their most recent SDP or of their most recent successfully completed security review,

e) to confirm compliance when one or more security breaches or incidents involving SSA-provided information occurred since approval of the EIEP's most recent SDP or of their most recent successfully completed security review,

f) to document descriptions and explanations of measures implemented as the result of a data breach or security incident,

g) to document descriptions and explanations of measures implemented to resolve non-compliancy issue(s), and

h) to obtain a new approval after SSA revoked approval of the most recent SDP

SSA may require a new SDP if changes occurred (other than those listed above) that may affect the terms of the EIEP's data exchange agreement with SSA.

SSA will not approve the SDP or allow the initiation of transactions and/or access to SSA-provided information before the EIEP complies with the TSSRs.

NOTE: EIEPs that function only as an STC, transferring SSA-provided information to other EIEPs must, per the terms of their agreements with SSA, adhere to SSA's TSSR and exercise their responsibilities regarding protection of SSA-provided information.
(See Page 48 Definition of STC)

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.3 The Certification Process
(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

Once the EIEP has successfully satisfied Phase 1, SSA will conduct an onsite certification review. The objective of the onsite review is to ensure the EIEP's management, operational, and technical controls safeguarding SSA-provided information from misuse and improper disclosure and that those safeguards function and work as intended.

At its discretion, SSA may request the EIEP to participate in an onsite review and compliance certification of their security infrastructure.

The onsite review may address any or all of SSA's security requirements and include, when appropriate:

1) a demonstration of the EIEP's implementation of each security requirement,

2) a physical review of pertinent supporting documentation to verify the accuracy of responses in the SDP,

3) a demonstration of the functionality of the software interface for the system that will receive, process, and store SSA-provided information,

4) a demonstration of the Automated Audit Trail System (ATS),

5) a walkthrough of the EIEP's data center to observe and document physical security safeguards,

6) a demonstration of the EIEP's implementation of electronic exchange of data with SSA,

7) a discussions with managers, supervisors, information security officers, system administrators, or other state stakeholders,

8) an examination of management control procedures and reports pertaining to anomaly detection or anomaly prevention,

9) a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,

10) a demonstration of the permission module or similar design, to show how the system triggers requests for information from SSA.

11) a demonstration of how the process for requests for SSA-provided information prevents SSNs not present in the EIEP's system from sending requests to SSA.

We may attempt to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEPs system.

During a certification or compliance review, SSA or a certifier acting on its behalf, may request a demonstration of the EIEP's ATS and its record retrieval capability. SSA or a certifier may request a demonstration of the ATS' capability to track the activity of employees who have the potential to access SSA-provided information within the EIEP's system. The certifier may request more information from those EIEPs who use an STC to handle and audit transactions. SSA or a certifier may conduct a demonstration to see how the EIEP obtains audit information from the STC regarding the EIEP's SSA transactions.

If an STC handles and audits an EIEP's transactions, SSA requires the EIEP to demonstrate both their in-house audit capabilities and the process used to obtain audit information from the STC.

If the EIEP employs a contractor or agent who processes, handles, or transmits the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include the contractor's facility in the onsite certification review. The inspection may occur with or without a representative of the EIEP.

Upon successful completion of the onsite certification review, SSA will authorize electronic access to production data by the EIEP. SSA will provide written notification of its certification to the EIEP and all appropriate internal SSA components.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.5 The Compliance Review Program and Process
(NIST SP 800-18 – System Security Plans, Configuration Management (CM), Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

Similar to the certification process, the compliance review program entails a process intended to ensure that EIEPs that receive electronic information from SSA are in full compliance with the SSA's TSSRs. SSA requires EIEPs to complete and submit (based on a timeline agreed upon by SSA and EIEP's stakeholders) a Compliance Review Questionnaire (CRQ). The CRQ (similar to the SDP), describes the EIEP's management, operational, and technical controls used to protect SSA-provided information from misuse and improper disclosure. We also want to verify that those safeguards function and work as intended.

As a practice, SSA attempts to conduct compliance reviews following a 3-5 year periodic review schedule. However, as circumstances warrant, a review may take place at any time. Three prominent examples that would trigger an ad hoc review are:

A. a significant change in the outside EIEP's computing platform,

B. a violation of any of SSA's TSSRs, or

C. an unauthorized disclosure of SSA-provided information by the EIEP.

SSA may conduct onsite compliance reviews and include both the EIEP's main facility and a field office.

SSA may, at its discretion, request that the EIEP participate in an onsite compliance review of their security infrastructure to confirm the implementation of SSA's security requirements.

The onsite review may address any or all of SSA's security requirements and include, where appropriate:

D. a demonstration of the EIEP's implementation of each requirement

E. a random sampling of audit records and transactions submitted to SSA

F. a walkthrough of the EIEP's data center to observe and document physical security safeguards

G. a demonstration of the EIEP's implementation of online exchange of data with SSA,

H. a discussion with managers, supervisors, information security officers, system administrators, or other state stakeholders,

I. an examination of management control procedures and reports pertaining to anomaly detection and prevention reports,

J. a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,

K. a demonstration of how a permission module or similar design triggers requests for information from SSA, and

L. a demonstration of how a permission module prevents the EIEP's system from processing SSNs not present in the EIEP's system.

1) **We can accomplish this by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEP's system.**

SSA may perform an onsite or remote review for reasons including, but not limited, to the following:

a) the EIEP has experienced a security breach or incident involving SSA-provided information

b) the EIEP has unresolved non-compliancy issue(s)

c) to review an offsite contractor's facility that processes SSA-provided information

d) the EIEP is a legacy organization that has not yet been through SSAs security certification and compliance review programs

e) the EIEP requested that SSA perform an IV & V (Independent Verification and Validation review)

During the compliance review, SSA, or a certifier acting on its behalf, may request a demonstration of the system's audit trail and retrieval capability. The certifier may request a demonstration of the system's capability for tracking the activity of employees who view SSA-provided information within the EIEP's system. The certifier may request EIEPs that have STCs that handle and audit transactions with SSA to demonstrate the process used to obtain audit information from the STC.

If an STC handles and audits the EIEP's transactions with SSA, we may require the EIEP to demonstrate both their in-house audit capabilities and the processes used to

obtain audit information from the STC regarding the EIEP's transactions with SSA.

If the EIEP employs a contractor who will process, handle, or transmit the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include in the onsite compliance review an onsite inspection of the contractor's facility. The inspection may occur with or without a representative of the EIEP. The format of the review in routine circumstances (e.g., the compliance review is not being conducted to address a special circumstance, such as a disclosure violation, etc.) will generally consist of reviewing and updating the EIEP's compliance with the systems security requirements described above in this document. At the conclusion of the review, SSA will issue a formal report to appropriate EIEP personnel. The Compliance Report will address findings and recommendations from SSA's compliance review, which includes a plan for monitoring each issue until closure.

NOTE: SSA will never request documentation for compliance reviews unless necessary to assess the EIEP's security posture. The information is only accessible to authorized individuals who have a need for the information as it relates to the EIEP's compliance with its electronic data exchange agreement with SSA and the associated system security requirements and procedures. SSA will not retain the EIEP's documentation any longer than required. SSA will delete, purge, or destroy the documentation when the retention requirement expires.

Compliance Reviews are either on-site or remote reviews. High-risk reviews must be onsite reviews, medium risk reviews are usually onsite, and low risk reviews may qualify for a remote review via telephone. The past performance of the entire state determines whether a review is onsite or remote **SSA determines a state's risk level based on the "high water mark principle."** If one agency is high risk, the entire state is high risk. The following is a high-level example of the analysis that aids SSA in making a preliminary determination as to which review format is appropriate. SSA may also use additional factors to determine whether SSA will perform an onsite or remote compliance review.

A. High/Medium Risk Criteria

1) undocumented closing of prior review finding(s),

2) implementation of management, operational or technical controls that affect security of SSA-provided information (e.g. implementation of new data access method), or

3) a reported PII breach within the state.

B. Low Risk Criteria

1) no prior review finding(s) or prior finding(s) documented as closed

2) no implementation of technical/operational controls that impact security of SSA provided

3) information (e.g. implementation of new data access method) no reported PII breach

6.5.1 EIEP Compliance Review Participation

SSA may request to meet with the following stakeholders during the compliance review:

a) a sample of managers, supervisors, information security officers, system administrators, etc. responsible for enforcing and monitoring ongoing compliance to security requirements and procedures to assess their level of training to monitor their employee's use of SSA-provided information, and for reviewing reports and taking necessary action

b) the individuals responsible for performing security awareness and employee sanction functions to learn how EIEPs fulfill this requirement

c) a sample of the EIEP's employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA-provided information

d) the individual(s) responsible for management oversight and quality assurance functions to confirm how the EIEP accomplishes this requirement

e) any additional individuals as deemed appropriate by SSA (i.e. analysts, Project/Program Manager, claims reps, etc.)

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.6 Scheduling the Onsite Review

SSA will not schedule the onsite review until SSA approves the EIEP's SDP or the EIEPs stakeholders participating in the compliance review have agreed upon a schedule. There is no prescribed period for arranging the subsequent onsite review (***certification review*** for an EIEP requesting initial access to SSA-provided information for an initial agreement or ***compliance review*** for other EIEPs). Unless there are compelling circumstances precluding it; the onsite review will occur as soon as reasonably possible.

The scheduling of the onsite review may depend on additional factors including:

a) the reason for submission of an SDP or CRQ,

b) the severity of security issues, if any,

c) circumstances of the previous review, if any, and

d) SSA's workload and resource considerations.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

7. Additional Definitions

Back Button:

Refers to a button on a web browser's toolbar, the *backspace button* on a computer keyboard, a programmed keyboard button or mouse button, etc., that returns a user to a previously visited web page or application screen.

Breach:

Refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where unauthorized persons have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording

Browsing:

Requests for or queries of SSA-provided information for purposes not related to the performance of official job duties

Choke Point:

The firewall between a local network and the Internet is a choke point in network security, because any attacker would have to come through that channel, which is typically protected and monitored.

Cloud Computing:

The term refers to Internet-based computing derived from the cloud drawing representing the Internet in computer network diagrams. Cloud computing providers deliver on-line and on-demand Internet services. Cloud Services normally use a browser or Web Server to deliver and store information.

Cloud Computing (NIST SP 800-145 Excerpt):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models,

Essential Characteristics:

On-demand self-service - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity - Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service - Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS) - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific

community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

---

1 Typically this is done on a pay-per-use or charge-per-use basis.

2 A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

3 This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

Cloud Drive:

A cloud drive is a Web-based service that provides storage space on a remote server.

Cloud Audit:

Cloud Audit is a specification developed at Cisco Systems, Inc. that provides cloud computing service providers a standard way to present and share detailed, automated statistics about performance and security.

The Federal Risk and Authorization Program (FedRAMP):
FedRAMP is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

Commingling:

Commingling is the creation of a common database or repository that stores and maintains both SSA-provided information and preexisting EIEP PII.

Data Exchange:

Data Exchange is a logical transfer of information from one government entity's systems of records (SOR) to another agency's application or mainframe through a secure and exclusive connection.

Degaussing:

Degaussing is the method of using a "special device" (i.e., a device that generates a magnetic field) in order to disrupt magnetically recorded information. Degaussing can be effective for purging damaged media and media with exceptionally large storage capacities. Degaussing is not effective for purging non-magnetic media (e.g., optical discs).

Function:

One or more persons or organizational components assigned to serve a particular purpose, or perform a particular role. The purpose, activity, or role assigned to one or more persons or organizational components.

Hub:

As it relates to electronic data exchange with SSA, a hub is an organization, which serves as an electronic information conduit or distribution collection point. The term Hub is interchangeable with the terms "StateTransmission Component," "State Transfer Component," or "STC."

ICON:

Interstate Connection Network (various entities use 'Connectivity' rather than 'Connection')

IV & V:

Independent Verification and Validation

Legacy System:

A term usually referring to a corporate or organizational computer system or network that utilizes outmoded programming languages, software, and/or hardware that typically no longer receives support from the original vendors or developers.

Manual Transaction:

A user-initiated operation (also referred to as a "user-initiated transaction"). This is the opposite of a system-generated automated process.

Example: A user enters a client's information including the client's SSN and presses the "ENTER" key to acknowledge that input of data is complete. A new screen appears with multiple options, which include "VERIFY SSN" and "CONTINUE". The user has the option to verify the client's SSN or perform alternative actions.

Media Sanitization:

f) Disposal: Refers to the discarding (e.g., recycling) media that contains no sensitive or confidential data.

g) Overwriting/Clearing: This type of media sanitization is adequate for protecting information from a robust keyboard attack. Clearing must prevent retrieval of information by data, disk, or file recovery utilities. Clearing must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. Deleting items, however, is not sufficient for clearing.

This process may include overwriting all addressable locations of the data, as well as its logical storage location (e.g., its file allocation table). The aim of the overwriting process is to replace or obfuscate existing information with random data. Most rewriteable media may be cleared by a single overwrite. This method of sanitization is not possible on un-writeable or damaged media.

h) Purging: This type of media sanitization is a process that protects information from a laboratory attack. The terms *clearing* and *purging* are sometimes synonymous. However, for some media, clearing is not sufficient for purging (i.e., protecting data from a laboratory attack). Although most re-writeable media requires a single overwrite, purging may require multiple rewrites using different characters for each write cycle.

This is because a laboratory attack involves threats with the capability to employ non-standard assets (e.g., specialized hardware) to attempt data recovery on media outside of that media's normal operating environment.

i) Degaussing is also an example of an acceptable method for purging magnetic media. The EIEP should destroy media if purging is not a viable method for sanitization.

- Destruction: Physical destruction of media is the most effective form of sanitization. Methods of destruction include burning, pulverizing, and shredding. Any residual medium should be able to withstand a laboratory attack.

Permission module:

A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA-provided information to an authorized process or transaction before initiating a transaction. The System will not allow a user to request information from SSA unless the EIEP's client system contains a record of the subject individual's SSN. A properly configured Permission Module also enforces referential integrity and prevents unauthorized random browsing of PII.

Screen Scraping:

Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This involves reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data.

A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

Security Breach:

An act from outside an organization that bypasses or violates security policies, practices, or procedures.

Security Incident:

A security incident happens when a fact or event signifies the possibility that a breach of security may be taking place, or may have taken place. All threats are security incidents, but not all security incidents are threats.

Security Violation:

An act from within an organization that bypasses or disobeys security policies, practices, or procedures.

Sensitive data:

Sensitive data is a special category of personally identifiable information (PII) that has the potential to cause great harm to an individual, government agency, or program if abused, misused, or breached. It is sensitive information protected against unwarranted disclosure and carries specific criminal and civil penalties for an individual convicted of unauthorized access, disclosure, or misuse. Protection of sensitive information usually involves specific classification or legal precedents that provide special protection for legal and ethical reasons.

Security Information Management (SIM):

SIM is software that automates the collection of event log data from security devices such as firewalls, proxy servers, intrusion detection systems and anti-virus software. The SIM translates the data into correlated and simplified formats.

SMDS (Switched Multimegabit Data Service (SMDS):

SMDS is a telecommunications service that provides connectionless, high-performance, packet- switched data transport. Although not a protocol, it supports standard protocols and communications interfaces using current technology.

SSA-provided data/information:

Synonymous with "SSA-supplied data/information", defines information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. The following are examples of SSA-provided data/information:

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)
- SSA's response to a query from an EIEP for verification of an SSN

SSA data/information:

This term, sometimes used interchangeably with "SSA-provided data/information," denotes information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. However, **"SSA data/information"** also includes information provided to the EIEP by a source other than SSA, but which the EIEP attests to that SSA verified it, or the EIEP couples the information with data from SSA as to to certify the accuracy of the information. The following are examples of SSA information:

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)
- SSA's response to a query from an EIEP for verification of an SSN

- Display by the EIEP of SSA's response to a query for verification of an SSN ***and*** the associated SSN provided by SSA
- Display by the EIEP of SSA's response to a query for verification of an SSN ***and*** the associated SSN provided to the EIEP by a source other than SSA
- Electronic records that contain only SSA's response to a query for verification of an SSN ***and*** the associated SSN whether provided to the EIEP by SSA or a source other than SSA

SSN:

Social Security Number

STC:

A State Transmission/Transfer Component is an organization, which performs as an electronic information conduit or collection point for one or more other entities (also referred to as a hub).

System-generated transaction:

A transaction automatically triggered by an automated system process.

Example: A user enters a client's information including the client's SSN on an input screen and presses the "ENTER" key to acknowledge that input of data is complete. An automated process then matches the SSN against the organization's database and when the systems finds no match, automatically sends an electronic request for verification of the SSN to SSA.

Systems process:

Systems Process refers to a software program module that runs in the background within an automated batch, online, or other process.

Third Party:

Third Party pertains to an entity (person or organization) provided access to SSA-provided information by an EIEP or other SSA business partner for which one or more of the following apply:

- is not stipulated access to SSA-provided information by an information-sharing agreement between an EIEP and SSA
- has no data exchange agreement with SSA
- SSA does not directly authorize access to SSA-provided information

Transaction-driven:

This term pertains to an automatically initiated online query of or request for SSA information by an automated transaction process (e.g., driver license issuance, etc.). The query or request will only occur the automated process meets prescribed conditions.

Uncontrolled transaction:

This term pertains to a transaction that falls outside a permission module. An uncontrolled transaction is not subject to a systematically enforced relationship between an authorized process or application and an existing client record.

8. Regulatory References

- Federal Information Processing Standards (FIPS) Publications
- Federal Information Security Management Act of 2002 (FISMA)
- Homeland Security Presidential Directive (HSPD-12)
- National Institute of Standards and Technology (NIST) Special Publications
- Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*
- Office of Management and Budget (OMB) Circular A-130, Appendix III, *Management of Federal Information Resources*
- Office of Management and Budget (OMB) Memo M-06-16, *Protection of Sensitive Agency Information, June 23, 2006*
- Office of Management and Budget (OMB) Memo M-07-16, *Memorandum for the Heads of Executive Departments and Agencies May 22, 2007*
- Office of Management and Budget (OMB) Memo M-07-17, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007*
- Privacy Act of 1974, as amended

9. Frequently Asked Questions (Click links for answers or additional information)

1. Q: What is a breach of data?
   A: Refer to Security Breach, Security Incident, and Security Violation.

2. Q: What is employee browsing?
   A: Requests for or queries of SSA-provided information for purposes not related to the performance of official job duties

3. Q: Okay, so the EIEP submitted the SDP. Can SSA schedule the Onsite

Review?
A: Refer to Scheduling the Onsite Review.

4. Q: What is a **"Permission Module**?"
A: A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA-provided information to an authorized process or transaction before initiating a transaction. For example, if requests for verification of an SSN for issuance of a driver's license happens automatically from within a state driver's license application. The System will not allow a user to request information from SSA unless the EIEP's client system contains a record of the subject individual's SSN.

5. Q: What **"Screen Scraping**?"
A: Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This involves reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data.

A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

6. Q: When does an EIEP have to submit an SDP?
A: Refer to When the SDP is Required.

7. Q: Does an EIEP have to submit an SDP when the agreement is renewed?
A: The EIEP does not have to submit an SDP ***because*** the agreement between the EIEP and SSA was renewed. There are, however, circumstances that require an EIEP to submit an SDP.
Refer to When the SDP is Required.

8. Q: Is it acceptable to save SSA-provided information with a verified indicator on a (EIEP) workstation if the EIEP uses an encrypted hard drive? If not, what options does the agency have?
A: There is no problem with an EIEP saving SSA-provided information on the encrypted hard drives of computers used to process SSA-provided information if the EIEP retains the information only as provided for in

the EIEP's data-sharing agreement with SSA.
Refer to Data and Communications Security.

9. Q: Does SSA allow EIEPs to use caching of SSA-provided information on the EIEP's workstations?
A: Caching during processing is not a problem. However, SSA-provided information must clear from the cache when the user exits the application. Refer to Data and Communications Security.

10. Q: What does the term "interconnections to other systems" mean?
A: As used in SSA's system security requirements document, the term "interconnections" is the same as the term "connections."

11. Q: Is it acceptable to submit the SDP as a .PDF file?
A: No, it is not. The document must remain editable.

12. Q: Should the EIEP write the SDP from the standpoint of the EIEP SVES (or applicable data element) access itself, or from the standpoint of access to all data provided to the EIEP by SSA?
A: The SDP is to encompass the EIEP's entire electronic access to SSA-provided information as per the electronic data exchange agreement between the EIEP and SSA.
Refer to Developing the SDP.

13. Q: If the EIEP has a "transaction-driven" system, does the EIEP still need a permission module? If employees cannot initiate a query to SSA, why would the EIEP need the permission module?
A: "Transaction driven" means that queries submit requests automatically (and it might depend on the transaction). Depending on the system's design, queries might not be automatic or it may still permit manual transactions. A system may require manual transactions to correct an error. SSA does not prohibit manual transactions if an ATS properly tracks such transactions. If a "transaction-driven" system permits any type of alternate access, it still requires a permission module, even if it restricts users from performing manual transactions. If the system does ***not*** require the user to be in a particular application and/or the query to be for an existing record in the EIEP's system ***before*** the system will allow a query to go through to SSA, it would still need a permission module.

14. Q: What is an Onsite Compliance Review?
A: The Onsite Compliance Review is SSA's periodic site visits to its Electronic Information Exchange Partners (EIEP) to certify whether the EIEP's management, operational, and technical security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEP's data sharing agreements with SSA and SSA's associated system security requirements and procedures.
Refer to the Compliance Review Program and Process.

15. Q: What are the criteria for performing an Onsite Compliance Review?
A: The following are criteria for performing the Onsite Compliance Review:

- EIEP initiating new access or new access method for obtaining information from SSA
- EIEP's cyclical review (previous review was performed remotely)
- EIEP has made significant change(s) in its operating or security platform involving SSA-provided information
- EIEP experienced a breach of SSA-provided personally identifying information (PII)
- EIEP has been determined to be high-risk

16. Q: What is a Remote Compliance Review?
A: The Remote Compliance Review is when SSA conducts the meetings remotely (e.g., via conference calls). SSA schedules conference calls with its EIEPs to determine whether the EIEPs technical, managerial, and operational security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEP's data sharing agreements with SSA and SSA's associated system security requirements and procedures. Refer to the Compliance Review Program and Process.

17. Q: What are the criteria for performing a Remote Compliance Review?
A: The EIEP must satisfy the following criteria to qualify for a Remote Compliance Review:

- EIEP's cyclical review (SSA's previous review yielded no findings or the EIEP satisfactorily resolved cited findings)
- EIEP has made no significant change(s) in its operating or security platform involving SSA-provided information
- EIEP has not experienced a breach of SSA-provided personally identifying information (PII) since its previous compliance review.
- SSA rates the EIEP as a low-risk agency or state

ATTACHMENT 5

SYSTEM CERTIFICATION REQUIREMENTS FOR THE CMS HUB

Not Applicable

Security Certification Requirements for use of the *SSA Data Set* via the Centers for Medicare & Medicaid Services' (CMS) Hub

The Social Security Administration (SSA) does not allow new data exchange partners to begin receiving data electronically until the Authorized State Agency submits an approved Security Design Plan (SDP). SSA's Office of Information Security (OIS) usually performs an onsite security review to verify and validate that the management, operational, and technical controls conform to the requirements of the signed agreements between SSA and the Authorized State Agency, as well as applicable Federal law and SSA's technical systems security requirements (Attachment 4 to the Information Exchange Agreement (IEA)). As it concerns the use of the *SSA Data Set* via the Hub, OIS will waive the initial SDP/Certification for an existing Authorized State Agency if it meets all the following criteria:

1. The Authorized State Agency already has a functioning CMS-approved Integrated Eligibility Verification System (IEVS).
2. The Authorized State Agency is already receiving data from the Hub to support the Medicaid program and/or the Children's Health Insurance Program (CHIP).
3. The Authorized State Agency will only process requests for the *SSA Data Set* for administration of health or income maintenance programs approved by SSA through the Hub in conjunction with Insurance Affordability Programs eligibility determinations.
4. The Authorized State Agency agrees that the SSA security controls identified in the IEA and Attachment 4 to the IEA will prevail for all SSA data received by the State Agency, including the *SSA Data Set*.
5. The Authorized State Agency agrees that a significant vulnerability or risk in a security control, a data loss, or a security breach may result in a suspension or termination of the *SSA Data Set* through the Hub. In this case, at SSA's request, the Authorized State Agency agrees to immediately cease using the *SSA Data Set* for all SSA authorized health or income maintenance programs until the State Agency sufficiently mitigates or eliminates such risk(s) and/or vulnerabilities to SSA's data.
6. The Authorized State Agency agrees not to process verification requests through the Hub from a standalone application for health or income maintenance program requests that have no connection to Insurance Affordability Programs eligibility determinations.

In the event that an Authorized State Agency decides to implement a new integrated eligibility system or use a different Authorized State Agency to implement the health or income maintenance data exchange process through the Hub, the Authorized State Agency will submit to SSA's OIS an SDP and be approved/certified prior to receipt of the *SSA Data Set* through the Hub. The Authorized State Agency will adhere to the following criteria, in addition to those stated in the IEA, section C, Program Questionnaire:

1. The Authorized State Agency agrees to provide an attestation to SSA that it has received certification through the CMS Hub approval MARS-E process.
2. The Authorized State Agency attests that it operates and has a CMS-approved IEVS and the IEVS initiates the request for the *SSA Data Set* for the State Agency's administration of health or income maintenance programs approved by SSA through the Hub in conjunction with Insurance Affordability Programs eligibility determinations.

3. The Authorized State Agency uses a streamlined multi-benefit application. The Authorized State Agency agrees not to process verification requests through the Hub from a standalone application for health or income maintenance program requests that have no connection to Insurance Affordability Programs eligibility determinations.
4. The Authorized State Agency will not request the *SSA Data Set* through the Hub until it has successfully begun using the Hub for administration of Insurance Affordability Programs eligibility determinations. SSA will begin sending the *SSA Data Set* to the Authorized State Agency after the State Agency verifies that the Hub process works, as required by the CMS Hub approval MARS-E process.
5. The Authorized State Agency agrees to participate in SSA's SDP/Certification process prior to transmitting requests for the *SSA Data Set* through the Hub and to participate in SSA's triennial security compliance reviews on an ongoing basis.
6. The Authorized State Agency agrees that a significant vulnerability or risk in a security control, a data loss, or a security breach may result in a suspension or termination of the *SSA Data Set* through Hub. In this case, at SSA's request, the Authorized State Agency agrees to immediately cease using the *SSA Data Set* for all SSA authorized health or income maintenance programs until the State Agency sufficiently mitigates or eliminates such risk(s) and/or vulnerabilities to SSA's data.

ATTACHMENT 6

WORKSHEET FOR REPORTING LOSS OR PORTENTIAL LOSS OF PERSONALLY INDETIFIABLE INFORMATION

ATTACHMENT 6

09/27/06

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information

1. Information about the individual making the report to the NCSC:

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
E-mail Address:					
Check one of the following:					
Management Official		Security Officer		Non-Management	

2. Information about the data that was lost/stolen:

Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

Name		Bank Account Info	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Info	
Place of Birth		Mother's Maiden Name	
Address		Other (describe):	

Estimated volume of records involved:

3. How was the data physically stored, packaged and/or contained?

Paper or Electronic? (circle one):

If Electronic, what type of device?

Laptop		Tablet		Backup Tape		Blackberry	
Workstation		Server		CD/DVD		Blackberry Phone #	
Hard Drive		Floppy Disk		USB Drive			
Other (describe):							

Additional Questions if Electronic:

	Yes	No	Not Sure
a. Was the device encrypted?			
b. Was the device password protected?			
c. If a laptop or tablet, was a VPN SmartCard lost?			
Cardholder's Name:			
Cardholder's SSA logon PIN:			
Hardware Make/Model:			
Hardware Serial Number:			

Additional Questions if Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted?			
e. Other circumstances:			

4. **If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NCSC (as listed in #1), information about this employee/contractor:**

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
E-mail Address:					

5. **Circumstances of the loss:**
   a. When was it lost/stolen?

   b. Brief description of how the loss/theft occurred:

   c. When was it reported to SSA management official (date and time)?

6. **Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)**

7. **Which reports have been filed? (include FPS, local police, and SSA reports)**

Report Filed	Yes	No	Report Number
Federal Protective Service			
Local Police			

	Yes	No
SSA-3114 (Incident Alert)		
SSA-342 (Report of Survey)		
Other (describe)		

8. **Other pertinent information (include actions under way, as well as any contacts with other agencies, law enforcement or the press):**