MAR - 4 2016

CONTRACTOR: Yolo County

AGREEMENT NUMBER: 14-90116 A03

14-90116 A03
Yolo County
Attn: County Program Administrator
137 North Cottonwood Street
Suite 2500
Woodland, CA 95695

Department of Health Care Services (DHCS) has standardized its agreement formats. The enclosed agreement may reference on-line terms and conditions (GTC or GIA) that are not attached to the agreement. If applicable, the cited terms may be viewed at this web site: http://www.ols.dgs.ca.gov/Standard+Language/default.htm. The enclosed agreement is not binding until signed by all parties and approved by the appropriate state agencies. No services should be provided prior to approval, as DHCS is not obligated to make any payments for services occurring prior to approval. Required action is noted by each checked [X] item below.

[ ] Affix a signature to the enclosed agreement copy and each face sheet. Two copies must bear original signatures. Return **all** copies to CMU's address noted below along with each item noted by a check mark [X]. A copy of the approved agreement will be distributed to you after it is fully executed. Alterations, in general, are not allowed. Alterations, if any, must be approved by the funding program and initialed by the person who signs the agreement.

[ ] Complete, sign, and return the Payee Data Record (STD 204). Payments cannot be issued without this form.

[ ] Go to http://www.ols.dgs.ca.gov/Standard+Language/default.htm, review the GTC version referenced on the face of the agreement as Exhibit C. Review provision 11 to locate the Contractor Certification Clause (CCC) version (i.e., 307) that applies. Read the CCC in its entirety. Sign the first page of the Certification. Return the first page of the originally signed Certification to the CMU address below. Failure to return the appropriate CCC version will prohibit DHCS from doing buisness with your firm.

[X] Enclosed for your records is a fully executed agreement copy. Include DHCS's agreement number on all invoices and future correspondence related to this agreement. Performance may commence.

[ ] The enclosed agreement has been signed by DHCS. When fully executed, **return one signed copy** to CMU's address below. Cite DHCS's agreement number on all correspondence about this agreement.

[ ] The enclosed agreement has been signed by DHCS and is fully executed. Cite the agreement number in future correspondence.

Contact CMU at (916) 650-0150 if there are questions about this letter. Return all items identified above to this address:

DHCS Contract Management Unit
MS 1403, 1501 Capitol Avenue
P.O. Box 997413
Sacramento, CA 95899-7413

For program matters, invoice/payment issues, or to discuss agreement alterations, contact:

Michael Reeves (916) 327-2696
DHCS Fiscal Management & Accountability
P.O. Box 997413, MS2624
Sacramento, CA 95899-7413

Enclosure(s)

STATE OF CALIFORNIA
STANDARD AGREEMENT AMENDMENT
STD. 213A_DHCS (Rev. 03/15)

☒ Check here if additional pages are added: 139 Page(s)

Agreement Number	Amendment Number
14-90116	A03
Registration Number:	

1. This Agreement is entered into between the State Agency and 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)
County of Yolo

2. The term of this Agreement is: July 1, 2014 through June 30, 2017

3. The maximum amount of this Agreement after this amendment is: $ 4,459,994 Four Million, Four Hundred Fifty Nine Thousand, Nine Hundred Ninety Four Dollars

4. The parties mutually agree to this amendment as follows. All actions noted below are by this reference made a part of the Agreement and incorporated herein:

I. **Amendment effective date:** July 1, 2016

II. **Purpose of amendment:** This amendment modifies the terms and conditions as outlined in the original contract.

III. Certain changes made in this amendment are shown as: Text additions are displayed in **bold and underline**. Text deletions are displayed as strike through text (i.e., ~~Strike~~).

(Continued on next page)

All other terms and conditions shall remain the same.

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.)*
County of Yolo

By *(Authorized Signature)* ✍ Joan Planell — Date Signed *(Do not type)* 2/16/16

Printed Name and Title of Person Signing
Joan Planell, Director, Yolo County Health and Human Services Agency

Address
~~625 Court Street, Room 204~~ 137 N. Cottonwood Street, Suite 2500
Woodland, CA 95695

STATE OF CALIFORNIA

Agency Name
Department of Health Care Services

By *(~~Authorized~~ Signature)* ✍ Don Rodriguez — Date Signed *(Do not type)* 3-3-16

Printed Name and Title of Person Signing
Don Rodriguez, Chief, Contract Management Unit

Address
1501 Capitol Avenue, Suite 71.5195, MS 1403, P.O. Box 997413,
Sacramento, CA 95899-7413

CALIFORNIA Department of General Services Use Only

☒ Exempt per: **DGS memo dated** 07/10/96 and Welfare and Institutions Code 14087.4

IV. Paragraph 4 (incorporated exhibits) on the face of the original STD 213 is amended to add the following revised exhibit.

Exhibit A A2– Scope of Work (2 pages)

All references to Exhibit A A1, in any exhibit incorporated into this agreement shall hereinafter be deemed to read Exhibit A A2. Exhibit A A1 is hereby replaced in its entirety by the attached revised exhibit.

V. Paragraph 4 (incorporated exhibits) on the face of the original STD 213 is amended to add the following revised exhibit.

Exhibit A Attachment I A2 – Program Specifications (42 pages)

All references to Exhibit A Attachment I A1, in any exhibit incorporated into this agreement shall hereinafter be deemed to read Exhibit A Attachment I A2. Exhibit A Attachment I A1 is hereby replaced in its entirety by the attached revised exhibit.

VI. Paragraph 4 (incorporated exhibits) on the face of the original STD 213 is amended to add the following revised exhibit.

Exhibit B A2 – Budget Detail and Payment Provisions (20 pages)

All references to Exhibit B A1, in any exhibit incorporated into this agreement shall hereinafter be deemed to read Exhibit B A2. Exhibit B A1 is hereby replaced in its entirety by the attached revised exhibit.

VII. Paragraph 4 (incorporated exhibits) on the face of the original STD 213 is amended to add the following revised exhibit.

Exhibit E A1 – Additional Provisions (4 pages)

All references to Exhibit E, in any exhibit incorporated into this agreement shall hereinafter be deemed to read Exhibit E A1. Exhibit E is hereby replaced in its entirety by the attached revised exhibit.

VIII. Paragraph 4 (incorporated exhibits) on the face of the STD 213 is amended to add the following revised exhibit:

Exhibit G, Attachment I A1– Social Security Administration Agreement (70 pages)

All references to Exhibit G Attachment I, in any exhibit incorporated into this agreement shall hereinafter be deemed to read Exhibit G, Attachment A1. Exhibit G, Attachment is hereby replaced in its entirety by the attached revised exhibit.

IX. All other terms and conditions shall remain the same.

Exhibit A A2
Scope of Work

1. Service Overview

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

State and the Contractor enter into this contract by authority of Chapter 3 of Part 1, Division 10.5 of the Health and Safety Code (HSC) and with approval of Contractor's County Board of Supervisors (or designee) for the purpose of providing alcohol and drug services. State and the Contractor identified in the Standard Agreement are the only parties to this Contract. This Contract is not intended, nor shall it be construed, to confer rights on any third party.

State and the Contractor enter into this contract for the purpose of identifying and providing for covered Drug Medi-Cal (DMC) services for substance use treatment in the Contractor's service area pursuant to Sections 11848.5(a) and (b) of the Health and Safety Code (hereinafter referred to as HSC), Sections ~~14124.20,~~ 14021.51 – 14021.53, and 14124.20 – 14124.25 of the Welfare and Institutions Code (hereinafter referred to as W&IC), and Title 22 of the California Code of Regulations (hereinafter referred to as Title 22), Sections 51341.1, 51490.1, and 51516.1.

State and the Contractor enter into this contract by authority of Title 45 of the Code of Federal Regulations Part 96 (45 CFR Part 96), Substance Abuse Prevention and Treatment Block Grants (SAPT Block Grant) for the purpose of planning, carrying out, and evaluating activities to prevent and treat substance abuse. **SAPT** Block Grant recipients must adhere to SAMHSA's National Outcome Measures (NOMs).

The objective is to make substance use treatment services available to Medi-Cal **and other non-DMC** beneficiaries through utilization of federal and state funds available pursuant to Title XIX and Title XXI of the Social Security Act **and the SAPT Block Grant** for reimbursable covered services rendered by certified DMC providers.

2. Service Location

The services shall be performed at applicable facilities in the County of Yolo.

3. Service Hours

The services shall be provided during the working hours and days as defined by the Contractor.

4. Project Representatives

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

Department of Health Care Services	**Contractor's/Grantee's Name**
Contract/Grant Manager: Mike Reeves Telephone: (916) 327-2696 Fax: (916) 322-1176 Email: Michael.reeves@dhcs.ca.gov	County Administrator Telephone: (530) 666-8550 Fax: (530) 666-3984

B. Direct all inquiries to:

Department of Health Care Services	**Contractor's/Grantee's Name**
Department of Health Care Services SUD PTRSD - FMAB Attention: Robert Strom Mail Station Code 2624 P.O. Box 997413 Sacramento, CA, 95899-7777 Telephone: (916) 327-2699 Fax: (916) 322-1176 Email: Robert.Strom@dhcs.ca.gov	~~Yolo County Department of Health Services~~ Attention: County AOD Program Administrator ~~625 Court Street, Room 204~~ Woodland, CA 95695 Telephone: ~~(530) 666-8550~~ Fax: ~~(530) 666-3984~~ please use address below:

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 Agreement.

5. See Exhibit A, Attachment I, for a detailed description of the services to be performed.

Yolo County Health and Human Services Agency
Attn: County AOD Program Administrator
137 N. Cottonwood Street, Suite 2500
Woodland, CA 95695

Telephone: (530)666-8651
Fax: (530)666-8294

Exhibit A, Attachment I A2
Program Specifications

Part I - General

A. Additional Contract Restrictions

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

B. Nullification of Drug Medi-Cal (DMC) Treatment Program substance use disorder services (if applicable)

The parties agree that if the Contractor fails to comply with the provisions of Welfare and Institutions Code (W&I) Section 14124.24, all areas related to the DMC Treatment Program substance use disorder services shall be null and void and severed from the remainder of this Contract.

In the event the Drug Medi-Cal Treatment Program Services component of this Contract becomes null and void, an updated Exhibit B, Attachment I ~~A2~~ I will take effect reflecting the removal of federal Medicaid funds and DMC State General Funds from this Contract. All other requirements and conditions of this Contract will remain in effect until amended or terminated.

C. Hatch Act

Contractor agrees to comply with the provisions of the Hatch Act (Title 5 USC, Sections 1501-1508), which limit the political activities of employees whose principal employment activities are funded in whole or in part with federal funds.

D. No Unlawful Use or Unlawful Use Messages Regarding Drugs

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

E. Noncompliance with Reporting Requirements

Contractor agrees that the State has the right to withhold payments until Contractor has submitted any required data and reports to the State, as identified in Exhibit A, Attachment I ~~A1~~, Part III – Reporting Requirements, or as identified in Document 1F(a), Reporting Requirements Matrix for Counties.

F. Limitation on Use of Funds for Promotion of Legalization of Controlled Substances

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

G. Restriction on Distribution of Sterile Needles

No Substance Abuse Prevention and Treatment (SAPT) Block Grant funds made available through this Contract shall be used to carry out any program ~~of distributing~~ **that includes the distribution of** sterile needles or syringes for the hypodermic injection of any illegal drug unless the State chooses to implement a demonstration syringe services program for injecting drug users.

H. Health Insurance Portability and Accountability Act (HIPAA) of 1996

If any of the work performed under this Contract is subject to the HIPAA, ~~then~~ Contractor shall perform the work in compliance with all applicable provisions of HIPAA. As identified in Exhibit G, the State and County shall cooperate to assure mutual agreement as to those transactions between them, to which this Provision applies. Refer to Exhibit G for additional information.

1. Trading Partner Requirements

(a) No Changes. Contractor hereby agrees that for the personal health information (Information), it will not change any definition, data condition or use of a data element or segment as proscribed in the federal HHS Transaction Standard Regulation. (45 CFR Part 162.915 (a))

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

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

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

2. Concurrence for Test Modifications to HHS Transaction Standards

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

3. Adequate Testing

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

4. Deficiencies

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

5. Code Set Retention

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

6. Data Transmission Log

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

I. Nondiscrimination and Institutional Safeguards for Religious Providers

Contractor shall establish such processes and procedures as necessary to comply with the provisions of Title 42, USC, Section 300x-65 and Title 42, CFR, Part 54, (Reference Document 1B).

J. Counselor Certification

Any counselor **or registrant** providing intake, assessment of need for services, treatment or recovery planning, individual or group counseling to participants, patients, or residents in a DHCS licensed or certified program is required to be certified as defined in Title 9, CCR, Division 4, Chapter 8. (Document 3H)

K. Cultural and Linguistic Proficiency

To ensure equal access to quality care by diverse populations, each service provider receiving funds from this contract shall adopt the federal Office of Minority Health Culturally and Linguistically Appropriate Service (CLAS) national standards (Document 3V).

L. Intravenous Drug Use (IVDU) Treatment

Contractor shall ensure that individuals in need of IVDU treatment shall be encouraged to undergo alcohol and other drug (AOD) treatment (42 USC 300x-23~~(b)~~ **(96.126(e))** ~~of PHS Act~~).

M. Tuberculosis Treatment

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

1. Routinely make available TB services to each individual receiving treatment for alcohol and other drug use and/or abuse;

2. Reduce barriers to patients' accepting TB treatment; and,

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

N. Trafficking Victims Protection Act of 2000

Contractor and its Subcontractors that provide services covered by this Contract shall comply with Section 106(g) of the Trafficking Victims Protection Act of 2000 ~~as amended~~ (22 U.S.C. 7104**(g)**) **as amended by section 1702**. For full text of the award term, go to: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title22-section7104d&num=0&edition=prelim

O. Tribal Communities and Organizations

Contractor shall regularly assess (e.g. review population information available through Census, compare to information obtained in CalOMS Treatment to determine whether population is being reached, survey Tribal representatives for insight in potential barriers) the substance use service needs of the American Indian/Alaskan Native (AI/AN) population within the County geographic area and shall engage in regular and meaningful consultation and collaboration with elected officials of the tribe, Rancheria, or their designee for the purpose of identifying issues/barriers to service delivery and improvement of the quality, effectiveness and accessibility of services available to AI/NA communities within the County.

P. Participation of County Alcohol and Drug Program Administrators Association of California and County Behavioral Health Director's Association of California.

Pursuant to HSC Section 11801(g), the ~~c~~**C**ounty AOD ~~p~~**P**rogram ~~a~~**A**dministrator shall participate and represent the ~~c~~**C**ounty in meetings of the County Alcohol and Drug Program Administrators Association of California for the purposes of representing the counties in their relationship with the State with respect to policies, standards, and administration for alcohol and other drug abuse services. Participation and representation shall also be provided by the County Behavioral Health Director's Association of California.

Pursuant to HSC Section 11811.5(c), the ~~c~~**C**ounty AOD ~~p~~**P**rogram ~~a~~**A**dministrator shall attend any special meetings called by the Director of DHCS. Participation and representation shall also be provided by the County Behavioral Health Director's Association of California.

Q. Youth Treatment Guidelines

Contractor will follow the guidelines in Document 1V, incorporated by this reference, "Youth Treatment Guidelines," in developing and implementing youth treatment programs funded under this Exhibit, until such time **a** new Youth Treatment Guideline are established and adopted. No formal amendment of this contract is required for new guidelines to ~~apply~~ **be incorporated into this contract**.

R. Perinatal Services Network Guidelines 2015

Pursuant to 45 CFR 96.124 ((c)(1-3)) the Contractor shall expend the specified percentage of SAPT Block Grant funds, as calculated by said regulations, on perinatal services, pregnant women, and women with dependent children each state fiscal year (SFY). The Contractor shall expend these funds either by establishing new programs or expanding the capacity of existing programs. The Contractor shall calculate the appropriate amount by using Generally Accepted Accounting Principles and the composition of the base shall be applied consistently from year to year. (See the County Share of SAPT Block Grant Women Services Expenditure Requirement Exhibit G)

Contractor shall comply with the perinatal program requirements as outlined in the Perinatal Services Network Guidelines 2015, promulgated pursuant to 45 under CFR

96.137. The "Perinatal Services Network Guidelines 2015" are attached to this contract as Document 1G, incorporated by reference, The contractor shall comply with the "Perinatal Services Network Guidelines 2015" until new Perinatal Services Network Guidelines are established and adopted. The incorporation of any new Perinatal Services Network Guidelines into this contract shall not require a formal amendment.

All SAPT BG-funded programs providing treatment services designed for pregnant women and women with dependent children will treat the family as a unit and therefore will admit both women and their children into treatment services, if appropriate.

The Contractor must directly provide, or provide a referral for, the following services:

1. **Primary medical care for women, including referral for prenatal care and, while the women are receiving such services, child care;**
2. **Primary pediatric care, including immunization, for their children;**
3. **Gender specific substance abuse treatment and other therapeutic interventions for women which may address issues of relationships, sexual and physical abuse and parenting, and child care while the women are receiving these services;**
4. **Therapeutic interventions for children in custody of women in treatment which may, among other things, address their developmental needs, their issues of sexual and physical abuse, and neglect; and**
5. **Sufficient case management and transportation to ensure that women and their children have access to services.**

~~R.~~**S.** Restrictions on Grantee Lobbying – Appropriations Act Section 503

No part of any appropriation contained in this Act shall be used, other than for formal and recognized executive-legislative relationships, for publicity or propaganda purposes, for the preparation, distribution, or use of any kit, pamphlet, booklet, publication, radio, television, or video presentation designed to support or defeat legislation pending before the Congress, except in presentation to the Congress or any State legislative body itself.

No part of any appropriation contained in this Act shall be used to pay the salary or expenses of any grant or contract recipient, or agent acting during for such recipient, related to any activity designed to influence legislation or appropriations pending before the Congress or any State legislature.

~~S.~~**T.** Nondiscrimination in Employment and Services

By signing this Contract, Contractor certifies that under the laws of the United States and the State of California, incorporated into this Contract by reference and made a part hereof as if set forth in full, Contractor will not unlawfully discriminate against any person.

~~T.~~**U.** Federal Law Requirements:

1. Title VI of the Civil Rights Act of 1964, Section 2000d, as amended, prohibiting discrimination based on race, color, or national origin in federally-funded programs.
2. Title VIII of the Civil Rights Act of 1968 (42 USC 3601 et seq.) prohibiting discrimination on the basis of race, color, religion, sex, handicap, familial status or national origin in the sale or rental of housing.
3. Age Discrimination Act of 1975 (45 CFR Part 90), as amended (42 USC Sections 6101 – 6107), which prohibits discrimination on the basis of age.
4. Age Discrimination in Employment Act (29 CFR Part 1625).
5. Title I of the Americans with Disabilities Act (29 CFR Part 1630) prohibiting discrimination against the disabled in employment.
6. Title II of the Americans with Disabilities Act (28 CFR Part 35) prohibiting discrimination against the disabled by public entities.
7. Title III of the Americans with Disabilities Act (28 CFR Part 36) regarding access.
8. Section 504 of the Rehabilitation Act of 1973, as amended (29 USC Section 794), prohibiting discrimination on the basis of ~~handicap~~ **individuals with disabilities**.
9. Executive Order 11246 (42 USC 2000(e) et seq. and 41 CFR Part 60) regarding nondiscrimination in employment under federal contracts and construction contracts greater than $10,000 funded by federal financial assistance.
10. Executive Order 13166 (67 FR 41455) to improve access to federal services for those with limited English proficiency.
11. The Drug Abuse Office and Treatment Act of 1972, as amended, relating to nondiscrimination on the basis of drug abuse.
12. The Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism.

~~U.~~**V.** State Law Requirements:

1. Fair Employment and Housing Act (Government Code Section 12900 et seq.) and the applicable regulations promulgated thereunder (California Administrative Code, Title 2, Section 7285.0 et seq.).
2. Title 2, Division 3, Article 9.5 of the Government Code, commencing with Section 11135.
3. Title 9, Division 4, Chapter 8 of the CCR, commencing with Section 10800.

4. No state or federal funds shall be used by the Contractor or its Subcontractors for sectarian worship, instruction, or proselytization. No state funds shall be used by the Contractor or its Subcontractors to provide direct, immediate, or substantial support to any religious activity.

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

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

~~W.~~**X.** Subcontract Provisions

Contractor shall include all of the foregoing provisions in all of its subcontracts.

Exhibit A, Attachment I A2
Program Specifications

Part II – Definitions

Section 1 - General Definitions.

The words and terms of this Contract are intended to have their usual meanings unless a particular or more limited meaning is associated with their usage pursuant to Division 10.5 of HSC, Section 11750 et seq., and Title 9, CCR, Section 9000 et seq.

A. **"Available Capacity"** means the total number of units of service (bed days, hours, slots, etc.) that a Contractor actually makes available in the current fiscal year.

B. **"Contractor"** means the county identified in the Standard Agreement or the department authorized by the County Board of Supervisors to administer substance use disorder programs.

C. **"Corrective Action Plan" (CAP)"** means the written plan of action document which the Contractor or its subcontracted service provider develops and submits to DHCS to address or correct a deficiency or process that is non-compliant with laws, regulations or standards.

D. **"County"** means the county in which the Contractor physically provides covered substance use treatment services.

E. **"County Realignment Funds"** means Behavioral Health Subaccount funds received by the ~~c~~County as per California Code Section 30025.

F. **"Days"** means calendar days, unless otherwise specified.

G. **"Dedicated Capacity"** means the historically calculated service capacity, by modality, adjusted for the projected expansion or reduction in services, which the Contractor agrees to make available to provide non-Drug Medi-Cal substance use disorder services to persons eligible for Contractor's services.

H. **"Final Allocation"** means the amount of funds identified in the last allocation letter issued by the State for the current fiscal year.

I. **"Final Settlement"** means permanent settlement of the Contractor's actual allowable costs or expenditures as determined at the time of audit, which shall be completed within three years of the date the year-end cost settlement report was accepted for interim settlement by the State. If the audit is not completed within three years, the interim settlement shall be considered as the final settlement.

J. **"Interim Settlement"** means temporary settlement of actual allowable costs or expenditures reflected in the Contractor's year-end cost settlement report.

K. **"Maximum Payable"** means the encumbered amount reflected on the Standard Agreement of this Contract and supported by Exhibit B, Attachment I ~~A2~~.

L. **"Modality"** means those necessary overall general service activities to provide substance use disorder services as described in Division 10.5 of the HSC.

M. **"Non-Drug Medi-Cal Amount"** means the contracted amount of SAPT Block Grant funds for services agreed to by the State and the Contractor.

N. **"Performance"** means providing the dedicated capacity in accordance with Exhibit B, Attachment I ~~A2~~, and abiding by the terms of this Exhibit, including all applicable state and federal statutes, regulations, and standards, including Alcohol and/or Other Drug Certification Standards (Document 1P), in expending funds for the provision of ~~alcohol and drug~~ **substance use** services hereunder.

O. **"Preliminary Settlement"** means the settlement of only SAPT funding for counties that do include DMC funding.

P. **"Revenue"** means Contractor's income from sources other than the State allocation.

Q. **"Service Area"** means the geographical area under Contractor's jurisdiction.

R. **"Service Element"** is the specific type of service performed within the more general service modalities. A list of the service modalities and service elements and service elements codes is incorporated into this Contract as Document 1H(a) "Service Code Descriptions".

S. **"State"** means the Department of Health Care Services or DHCS.

T. **"Utilization"** means the total actual units of service used by clients and participants.

Section 2 – Definitions Specific to Drug Medi-Cal

The words and terms of this Contract are intended to have their usual meaning unless a specific or more limited meaning is associated with their usage pursuant to the HSC, Title ~~96~~, and/or Title 22. Definitions of covered treatment modalities and services are found in Title 22 (Document 2C) and are incorporated by this reference.

A. **"Administrative Costs"** means the Contractor's actual direct costs, as recorded in the Contractor's financial records and supported by source documentation, to administer the program or an activity to provide service to the DMC program. Administrative costs do not include the cost of treatment or other direct services to the beneficiary. Administrative costs may include, but are not limited to, the cost of training, programmatic and financial audit reviews, and activities related to billing. Administrative costs may include Contractor's overhead per the approved indirect cost rate proposal pursuant to OMB Circular A-87 and the State Controller's Office Handbook of Cost Plan Procedures.

B. **"Authorization"** is the approval process for DMC Services prior to the submission of a DMC claim.

C. **"Beneficiary"** means a person who: (a) has been determined eligible for Medi-Cal; (b) is not institutionalized; (c) has a substance-related disorder per the "Diagnostic and Statistical Manual of Mental Disorders III Revised (DSM)," and/or DSM IV criteria; and (d) meets the admission criteria to receive DMC covered services.

D. **"Certified Provider"** means a substance use disorder clinic and/or satellite clinic location that has received certification to be reimbursed as a DMC clinic by the State to provide services as described in Title 22, California Code of Regulations, Section 51341.1.

E. **"Covered Services"** means those DMC services authorized by Title XIX or Title XXI of the Social Security Act; Title 22 Section 51341.1; W&I **Code,** Section 14124.24; and California's Medicaid State Plan.

F. **"Direct Provider Contract"** means a contract established between the State and a Drug Medi-Cal certified provider entered into pursuant to this Agreement for the provision of Drug Medi-Cal services.

G. **"Drug Medi-Cal Program"** means the state system wherein beneficiaries receive covered services from DMC-certified substance use disorder treatment providers.

H. **"Drug Medi-Cal Termination of Certification"** means the provider is no longer certified to participate in the Drug Medi-Cal program upon the State's issuance of a Drug Medi-Cal certification termination notice.

I. **"Early and Periodic Screening, Diagnosis, and Treatment Program (EPSDT)"** means the federally mandated Medicaid benefit that entitles full-scope Medi-Cal-covered beneficiaries less than 21 years of age to receive any Medicaid service necessary to correct or ameliorate a defect, mental illness, or other condition, such as a substance-related disorder~~,~~ that is discovered during a health screening.

J. **"Provider Certification"** means the provider must be certified in order to participate in the Medi-Cal program.

K. **"Federal Financial Participation (FFP)"** means the share of federal Medicaid funds for reimbursement of DMC services.

L. **"Medical Necessity"** means those substance use treatment services that are reasonable and necessary to protect life, prevent significant illness or disability, or alleviate severe pain through the diagnosis and treatment of a disease, illness, or injury, or, in the case of EPSDT, services that meet the criteria specified in Title 22, Sections 51303 and 51340.1.

M. **"Minor Consent DMC Services"** are those covered services that, pursuant to Family Code Section 6929, may be provided to persons 12-20 years old without parental consent.

N. **"Narcotic Treatment Program"** means an outpatient clinic licensed by the State to provide narcotic replacement therapy directed at stabilization and rehabilitation of persons who are opiate-addicted and have a substance use diagnosis.

O. **"Payment Suspension"** means the Drug Medi-Cal certified provider has been issued a notice pursuant to W&I **Code, Section** 14107.11 and is not authorized to receive payments after the payment suspension date for DMC services, regardless of when the service was provided.

P. **"Perinatal DMC Services"** means covered services as well as mother/child habilitative and rehabilitative services; services access (i.e., provision or arrangement of transportation to and from medically necessary treatment); education to reduce harmful effects of alcohol and drugs on the mother and fetus or infant; and coordination of ancillary services (Title 22, Section 51341.1(c) 4).

Q. **"Postpartum"**, as defined for DMC purposes, means the 60-day period beginning on the last day of pregnancy, regardless of whether other conditions of eligibility are met. Eligibility shall end on the last day of the calendar month in which the 60th day occurs.

R. **"Post Service Post Payment (PSPP) Utilization Review"** means the review for program compliance and medical necessity conducted by the State after service was rendered and paid. State may recover prior payments of Federal and State funds if such review determines that the services did not comply with the applicable statutes, regulations, or standards (CCR, Title 22, Section 51341.1 **(k)**).

S. **"Projected Units of Service"** means the number of reimbursable DMC units of service, based on historical data and current capacity, the Contractor expects to provide on an annual basis.

T. **"Provider of DMC Services"** means any person or entity that provides direct substance use treatment services and has been certified by **the** State as meeting the standards for participation in the DMC program set forth in the "DMC Certification Standards for Substance Abuse Clinics", Document 2E and "Standards for Drug Treatment Programs (October 21, 1981)", Document 2F.

U. **"Re-certification"** means the process by which the **DMC** certified clinic and/or satellite program is required to submit an application and specified documentation, as determined by DHCS, to remain eligible to participate in and be reimbursed in through the DMC program. Re-certification shall occur no less than every five years from **the** date of previous DMC certification or re-certification.

V. **"Statewide Maximum Allowances (SMA)"** means the maximum amount authorized to be paid by DMC for each covered unit of service for outpatient drug free, intensive outpatient treatment, perinatal residential, and Naltrexone treatment services. While the rates are approved by the State, they are subject to change through the regulation process. The SMA for FY ~~2015-16~~**2016-17** is listed in the "Unit of Service" table in Exhibit B ~~A1~~, Part V.

W. **"Subcontract"** means an agreement between the Contractor and its Subcontractors. A Subcontractor shall not delegate its obligation to provide covered services or otherwise subcontract for the provision of direct patient/client services.

X. **"Subcontractor"** means an individual or entity that is DMC certified and has entered into an agreement with the Contractor to be a provider of covered services. It may also mean a vendor who has entered into a procurement agreement with the Contractor to provide any of the administrative functions related to fulfilling the Contractor's obligations under the terms of this Exhibit A, Attachment I ~~A1~~.

Y. **"Temporary Suspension"** means the provider is temporarily suspended from participating in the DMC program as authorized by W&I **Code,** Section 14043.36(a). The provider cannot bill for DMC services from the effective date of the temporary suspension.

Exhibit A, Attachment I A2
Program Specifications

Part III – Reporting Requirements

Contractor agrees that the State has the right to withhold payments until Contractor has submitted any required data and reports to the State, as identified in this Exhibit A, Attachment I ~~A1~~ or as identified in Document 1F (a), Reporting Requirement Matrix for Counties.

A. Quarterly Federal Financial Management Report (QFFMR)

The QFFMR must be submitted to reflect quarterly SAPT_BG expenditures.

For the beginning of each federal award year, the due dates are:

March 1 for the period October through December
June 1 for the period January through March
September 1 for the period April through June
December 1 for the period July through September

B. Year-End Cost Settlement Reports

Pursuant to W&I **Code,** Section 14124.24 **(g(1))** Contractor shall submit to the State, on November 1 of each year, the following year-end cost settlement documents by paper or electronic **format**, as prescribed by the State, submission for the previous fiscal year:

1. Document 2P, County Certification Year-End Claim for Reimbursement

2. Document 2P(a) and 2P(b), Drug Medi-Cal Cost Report Forms for Intensive Outpatient Treatment for Non-Perinatal or Perinatal (if applicable)

3. Document 2P(c) and 2P(d), Drug Medi-Cal Cost Report Forms for Outpatient Drug Free Individual Counseling for Non-Perinatal or Perinatal (if applicable)

4. Document 2P(e) and 2P(f), Drug Medi-Cal Cost Report Forms for Outpatient Drug Free Group Counseling for Non-Perinatal or Perinatal (if applicable)

5. Document 2P(g), Drug Medi-Cal Cost Report Forms for Residential for Perinatal (if applicable)

6. Document 2P(h) and 2P(i), Drug Medi-Cal Expenditure Forms for Narcotic Treatment Programs, ~~for~~ Non-Perinatal or Perinatal (if applicable)

C. Drug Medi-Cal Claims and Reports

Contractors or providers that bill the State or the County for services identified in Section 51516.1 of Title 22 shall submit claims in accordance with the Department of Health Care Services DMC Provider Billing Manual.

Contractors and Subcontractors that provide DMC services shall be responsible for verifying the Medi-Cal eligibility of each client for each month of service prior to billing for DMC services to that client for that month. Medi-Cal eligibility verification should be performed prior to rendering service, in accordance with and as described in the Department of Health Care Services DMC Provider Billing Manual. Options for verifying the eligibility of a Medi-Cal beneficiary are described in the Department of Health Care Services DMC Provider Billing Manual.

Claims for DMC reimbursement shall include only those services covered under Title 22, Section 51341.1(c-d) and administrative charges that are allowed under W&I C**ode**, Sections 14132.44 and 14132.47.

1. Contractor shall ~~certify the public expenditure~~ **submit the "Certified Expenditure" form** reflecting **either: 1)** the approved amount of the 837P claim file**, after the claims have been adjudicated; or 2) the claimed amount identified on the 837P claim file, which could account for both approved and denied claims.** Contractor shall submit ~~the "Certified Public Expenditure" form after the claims have been adjudicated Contractor shall submit~~ to the State the Drug Medi-Cal Certification Form DHCS Form DHCS 100224A (Document 4D) for each ~~835~~ **837P** transaction approved for reimbursement of the federal Medicaid funds.

2. DMC service claims shall be submitted electronically in a Health Insurance Portability and Accountability Act (HIPAA) compliant format (837P). All adjudicated claim information must be retrieved by the Contractor via an 835 HIPAA compliant format (Health Care Claim Payment/Advice).

3. The following forms shall be prepared as needed and retained by the provider for review by State staff:

   (a) Multiple Billing Override Certification (MC 6700), Document 2K

   (b) Good Cause Certification (6065A), Document 2L(a)

   (c) Good Cause Certification (6065B), Document 2L(b)

   In the absence of good cause documented on the Good Cause Certification (6065A or 6065B) form, claims that are not submitted within 30 days of the end of the month of service shall be denied. The existence of good cause shall be determined by the State in accordance with Title 22, CCR, Sections 51008 and 51008.5.

4. Certified Public Expenditure County Administration

   Separate from direct service claims as identified in #2 above, county may submit an invoice for administrative costs for administering the DMC program on a quarterly basis. The form requesting reimbursement shall be submitted to DHCS.

5. If while completing the Utilization Review and Quality Assurance requirements of this Exhibit A, Attachment I ~~A1~~, Part V, Section 4 any of the Contractor's skilled professional medical and personnel ~~and~~ directly supporting staff meet the criteria set forth in 42 C.F.R. 432.50(d)(1), then the Contractor shall submit a written request that specifically demonstrates how the skilled professional medical personnel and directly supporting staff meet all of the applicable criteria set forth in 42 C.F.R. 432.50(d)(1) and outlines the duties they will perform to assist the Department, or the Department's skilled professional medical personnel, in activities that are directly related to the administration of the Drug Medi-Cal Program. The Department shall respond to the Contractor's written request within 20 days with either a written agreement pursuant to 42 C.F.R. 432.50(d) (2) approving the request, or a written explanation as to why the Department does not agree that the Contractor's skilled professional medical personnel and directly supporting staff do not meet the criteria set forth in 42 C.F.R. 432.50(d) (1).

D. California Outcomes Measurement System (CalOMS) for Treatment (CalOMS-Tx)

The CalOMS-Tx business rules and requirements are:

1. Contractor **shall** contracts with a software vendor that complies with the CalOMS-Tx data collection system requirements for submission of CalOMS-Tx data. A Business Associate Agreement (BAA) **shall** ~~must~~ be established between the Contractor and the software vendor. The BAA **shall** ~~must~~ state that DHCS is allowed to return the processed CalOMS-Tx data to the vendor that supplied the data to DHCS.

2. Contractor shall conduct information technology (IT) systems testing and pass State certification testing before commencing submission of CalOMS-Tx data. If the Contractor subcontracts with vendor for IT services, Contractor is responsible for ensuring that the subcontracted IT system is tested and certified by the DHCS prior to submitting CalOMS-Tx data. If Contractor changes or modifies the CalOMS-Tx IT system, then Contractor shall re-test and pass state re-certification prior to submitting data from new or modified system.

3. Electronic submission of CalOMS-Tx data **shall be submitted by Contractor within** ~~is due~~ 45 days from the end of the last day of the report month.

4. Contractor shall comply with data collection and reporting requirements established by the DHCS CalOMS-Tx Data Collection Guide (Document 3J) and all former Department of Alcohol and Drug Programs Bulletins and DHCS Information Notices relevant to CalOMS-Tx data collection **and reporting requirements.** .

5. Contractor shall submit CalOMS-Tx admission, discharge, annual update, resubmissions of records containing errors or in need of correction, and "provider no activity" report records in an electronic format approved by DHCS.

6. Contractor shall comply with the CalOMS-Tx Data Compliance Standards established by DHCS identified in Document 3S for reporting data content, data quality, data completeness, reporting frequency, reporting deadlines, and reporting method.

7. Contractor shall participate in CalOMS-Tx informational meetings, trainings, and conference calls.

8. Contractor shall implement and maintain a system for collecting and electronically submitting CalOMS-Tx data.

9. Contractor shall meet the requirements as identified in Exhibit G, Privacy and Information Security Provisions and Exhibit G, Attachment I – SSA Agreement 2014.

E. California Outcomes Measurement Service for Prevention (CalOMS-Pv)

The CalOMS-Pv Business Rules and Requirements are:

1. Contractors and/or Subcontractors receiving Substance Abuse Prevention and Treatment (SAPT) Primary Prevention Set-Aside funding **shall** ~~must~~ input planning, service/activity and evaluation data into CalOMS Pv. When submitting data, Contractor ~~must~~ **shall** comply with the CalOMS Pv Data Quality Standards (Document #1T).

2. Contractor ~~must~~ **shall** report services/activities by the date of occurrence on an ongoing basis throughout each month. Contractor shall submit all data for each month no later than the 10th day of the following month.

3. Contractor ~~must~~ **shall** review all data input into CalOMS Pv on a quarterly basis. Contractor shall verify that the data meets the CalOMS Pv Data Quality Standards by reviewing and releasing the data. Certification is due by the last day of the month following the end of the quarter.

4. Contractor ~~must~~ **shall** report progress to DHCS via CalOMS Pv for the goals and objectives in the County Strategic Prevention Plan (as described in Exhibit A, Attachment 1 ~~A1~~, Part IV, Section 1B. 2) on an annual basis by September 30th of each fiscal year.

5. If Contractor cannot meet the established due dates, a written request for an extension ~~must~~ **shall** be submitted to DHCS 10 days prior to the due date

6. In order to ensure that all persons responsible for CalOMS Pv data entry have sufficient knowledge of the CalOMS Pv Data Quality Standards, all new CalOMS Pv users, whether employed by the Contractor or its Subcontractors, shall participate in CalOMS Pv trainings prior to inputting data into the system.

F. CalOMS-Tx and CalOMS-Pv General Information

1. If the Contractor experiences system or service failure or other extraordinary circumstances that affect its ability to timely submit CalOMS-Tx and/or CalOMS-Pv data, and or meet other CalOMS-Tx and/or CalOMS-Pv data compliance requirements, Contractor shall report the problem in writing before the established data submission deadlines. The written notice shall include a remediation plan that is subject to review and approval by the State. A grace period of up to sixty (60) days may be granted, at the State's sole discretion, for the Contractor to resolve the problem before non-DMC payments are withheld.

2. If the State experiences system or service failure, no penalties will be assessed to the Contractor for late data submission.

3. Contractor shall comply with the treatment and prevention data quality standards established by the State. Failure to meet these standards on an ongoing basis may result in withholding non-DMC funds.

4. If the Contractor submits data after the established deadlines, due to a delay or problem, Contractor is still responsible for collecting and reporting data from time of delay or problem.

G. Drug and Alcohol Treatment Access Report (DATAR)

The DATAR business rules and requirements are:

1. The Contractor shall be responsible for ensuring that the Contractor-operated treatment services and all treatment providers, with whom Contractor makes a contract or otherwise pays for the services, submit a monthly DATAR report in an electronic copy format as provided by the State.

   In those instances where the Contractor maintains, either directly or indirectly, a central intake unit or equivalent which provides intake services including a waiting list, the Contractor shall identify and begin submitting monthly DATAR reports for the central intake unit by a date to be specified by the State.

2. The Contractor shall ensure that all DATAR reports are submitted by either Contractor-operated treatment services and by each subcontracted treatment provider to the State by the 10th of the month following the report activity month.

3. The Contractor shall ensure that all applicable providers are enrolled in the State's web-based DATARWeb program for submission of data, accessible on the DHCS website when executing the subcontract.

4. If the Contractor or its Subcontractor experiences system or service failure or other extraordinary circumstances that affect its ability to timely submit a monthly DATAR report, and/or to meet data compliance requirements, the Contractor shall report the problem in writing before the established data submission deadlines. The written

notice shall include a corrective action plan that is subject to review and approval by the State. A grace period of up to sixty (60) days may be granted, at the State's sole discretion, for the Contractor to resolve the problem before non-DMC payments are withheld (See Exhibit B ~~A1~~, Part II, Section 2).

5. If the State experiences system or service failure, no penalties will be assessed to Contractor for late data submission.

6. The Contractor shall be considered compliant if a minimum of 95% of required DATAR reports from the Contractor's treatment providers are received by the due date.

H. Charitable Choice

Contractor shall ~~submit annually~~ **document** the total number of referrals necessitated by religious objection to other alternative substance abuse providers. **The contractor shall annually submit** ~~T~~this information ~~must be submitted~~ to DHCS **by October 1st. The annual submission shall contain all substantive information required by DHCS and be formatted in a manner** ~~in a format~~ prescribed by DHCS. ~~and at a time required by DHCS (reference ADP Bulletin 04-5).~~

I. Subcontractor Documentation

Contractor shall require its Subcontractors that are not licensed or certified by the State to submit organizational documents to the State within thirty (30) days of ~~its~~ **the** execution of an initial subcontract, within ninety (90) days of the renewal or continuation of an existing subcontract or when there has been a change in Subcontractor name or ownership. Organizational documents shall include the Subcontractor's Articles of Incorporation or Partnership Agreements (as applicable), and business licenses, fictitious name permits, and such other information and documentation as may be requested by the State.

J. Failure to meet required reporting requirements shall result in:

1. The DHCS will issue a Notice of Deficiency (Deficiencies) to Contractor regarding specified providers with a deadline to submit the required data and a request for a Corrective Action Plan (CAP) to ensure timely reporting in the future. The State will approve or reject the CAP or request revisions to the CAP which shall be resubmitted to the State within thirty (30) days.

2. If the Contractor has not ensured compliance with the data submission or CAP request within the designated timeline, then the State may withhold funds until all data is submitted. The State shall inform the Contractor when funds will be withheld.

Exhibit A, Attachment I A2
Program Specifications

PART IV – Non-Drug Medi-Cal Substance Use Disorder Prevention and Treatment Services

Section 1. General Provisions

A. Restrictions on Salaries

Contractor agrees that no part of any federal funds provided under this Contract shall be used by the Contractor or its Subcontractors to pay the salary and wages of an individual at a rate in excess of Level I of the Executive Schedule. Salary and wages schedules may be found at http://www.opm.gov/oca. SAPT Block Grant funds used to pay a salary in excess of the rate of basic pay for Level I of the Executive Schedule shall be subject to disallowance. The amount disallowed shall be determined by subtracting the individual's actual salary from the Level I rate of basic pay and multiplying the result by the percentage of the individual's salary that was paid with SAPT Block Grant funds (Reference: Terms and Conditions of the SAPT Block Grant award.)

B. Primary Prevention

1. The SAPT Block Grant regulation defines "Primary Prevention Programs" as those programs directed at "individuals who have not been determined to require treatment for substance abuse" (45 CFR 96.121). Primary Prevention includes strategies, programs and initiatives which reduce both direct and indirect adverse personal, social, health, and economic consequences resulting from problematic AOD availability, manufacture, distribution, promotion, sales, and use. The desired result of primary prevention is to promote safe and healthy behaviors and environments for individuals, families and communities. The Contractor shall expend not less than its allocated amount of the SAPT Block Grant on primary prevention as described in the SAPT Block Grant requirements (45 CFR 96.125). ~~Inappropriate use of these funds for non-primary prevention services will require repayment of SAPT Block Grant funds.~~

2. Contractor is required to have a current and DHCS approved County Strategic Prevention Plan (SPP). The SPP must demonstrate that the County utilized the Substance Abuse and Mental Health Services Administration's Strategic Prevention Framework (SPF) in developing the plan as described at http://captus.samhsa.gov/access-resources/about-strategic-prevention-framework-spf. DHCS will only approve SPP's that demonstrate that the Contractor utilized the SPF. Contractor must:

   a) Follow the DHCS guidelines provided in the Strategic Prevention Framework Plan Resource Document located in the CalOMS Pv Library.
   b) Begin preparing a new SPP at least 9-months prior to the expiration date of the current SPP.

c) Submit a timeline to DHCS for completion of the SPP that includes proposed dates for submitting each section of the SPP. The sections are outlined in the Strategic Prevention Framework Plan Resource Document.
d) Submit a draft to DHCS, based on the timeline~~,~~ for each section of the SPP for review and approval.
e) Submit to DHCS the final draft of the SPP no later than 30-days prior to the start date of the new SPP.
f) Upload an electronic copy of the approved SPP into CalOMS Pv within 10-days of approval.
g) Input the Problem Statements, Goals and Objectives from the SPP into CalOMS Pv no later than 10-days after the start date of the SPP.

3. Contractor shall submit a Prevention Mid-Year Budget to DHCS by January 31 of each fiscal year. The budget shall indicate how the SAPT Block Grant Primary Prevention Set-Aside will be expended for the fiscal year.

4. Friday Night Live

Contractors and Subcontractors receiving SAPT Friday Night Live (FNL) funding must:

(a) Engage in programming that meets the FNL Youth Development Standards of Practice, Operating Principles and Core Components outlined at http://fridaynightlive.org/about-us/cfnlp-overview/;
(b) Use CalOMS Pv for all FNL reporting including Chapter Profiles, FNL County Profiles and chapter activity;
(c) Follow the FNL Data Entry Instructions for ~~CAlOMS~~ **CalOMS** Pv as provided by DHCS in the CalOMS Pv Library;
(d) ~~Demonstrate an effort to be a~~ **Meet the** Member in Good Standing (MIGS) **requirements**, as ~~provided~~ **determined** by DHCS in conjunction with the California Friday Night Live Partnership. **If the Contractor does not meet the MIGS requirements, then the Contractor shall submit counties fail to a technical assistance plan detailing how the Contractor intends to ensure satisfaction of the MIGS requirements to DHCS for approval.**

C. Perinatal Services Network Guidelines ~~2014~~ **2015**

Pursuant to 45 CFR 96.124 ((c)(1-3)) the Contractor shall expend the specified percentage of SAPT Block Grant funds, as calculated by said regulations, on perinatal services, pregnant women, and women with dependent children each state fiscal year (SFY) . The Contractor shall expend these funds either by establishing new programs or expanding the capacity of existing programs. The Contractor shall calculate the appropriate expenditure amount by using Generally Accepted Accounting Principles and the composition of the base shall be applied consistently from year to year. (See the County Share of SAPT Block Grant Women Services Expenditure Requirement Exhibit G)

Contractor shall comply with the ~~requirements for~~ perinatal programs **requirements as outlined in the Perinatal Services Network Guidelines, promulgated to 45 CFR 96.137.**

The "Perinatal Services Network Guidelines 2015" ~~funded under under Exhibit A, Attachment I A1, contained in~~ **are attached to this contract as** Document 1G, incorporated by ~~this~~ reference. **The Contractor shall comply with the** "Perinatal Services Network Guidelines ~~2014~~ **2015**" until ~~such time~~ **new** Perinatal Services Network Guidelines are established and adopted. **The incorporation of any new Perinatal Service Netork Guidelines into this contract shall not require a** ~~No~~ formal amendment ~~of this contract is required for new guidelines to apply~~.

All SAPT BG-funded programs providing treatment services designed for pregnant women and women with dependent children will treat the family as a unit and therefore will admit both women and their children into treatment services, if appropriate.

The Contractor must directly provide, or provide a referral for the following services:

1. **Primary medical care for women, including referral for prenatal care and, while the women are receiving such services, child care;**
2. **Primary pediatric care, including immunization, for their children;**
3. **Gender specific substance abuse treatment and other therapeutic interventions for women which may address issues of relationships, sexual and physical abuse and parenting, and child care while the women are receiving these services;**
4. **Therapeutic interventions for children in custody of women in treatment which may, among other things, address their developmental needs, their issues of sexual and physical abuse, and neglect; and**
5. **Sufficient case management and transportation to ensure that women and their children have access to services.**

D. Funds identified in this contract shall be used exclusively for county alcohol and drug abuse services to the extent activities meet the requirements for receipt of federal block grant funds for prevention and treatment of substance abuse described I subchapter XVII of Chapter 6A of Title 42 of the United State Code. ~~(Health and Safety Code section 18100 et. seq.)~~

Section 2 – Formation and Purpose

A. Authority

State and the Contractor enter into this Exhibit A, Attachment I ~~A1~~, Part IV, by authority of Chapter 3 of Part 1, Division 10.5 of the Health and Safety Code (HSC) and with approval of Contractor's County Board of Supervisors (or designee) for the purpose of providing alcohol and drug services, which will be reimbursed pursuant to Exhibit A, Attachment I ~~A1~~. State and the Contractor identified in the Standard Agreement are the only parties to this Contract. This Contract is not intended, nor shall it be construed, to confer rights on any third party.

B. Control Requirements

1. Performance under the terms of this Exhibit A, Attachment I ~~A1~~, Part IV, is subject to all applicable federal and state laws, regulations, and standards. In accepting the State drug and alcohol combined program allocation pursuant to HSC Sections 11814(a) and (b), Contractor shall: (i) establish, and shall require its Subcontractors to establish, written policies and procedures consistent with the following requirements; (ii) monitor for compliance with the written procedures; and (iii) be held accountable for audit exceptions taken by the State against the Contractor and its Subcontractors for any failure to comply with these requirements:

   (a) HSC, Division 10.5, commencing with Section 11760;

   (b) Title 9, California Code of Regulations (CCR) (herein referred to as Title 9), Division 4, commencing with Section 9000;

   (c) Government Code Section 16367.8;

   (d) Government Code, Article 7, Federally Mandated Audits of Block Grant Funds Allocated to Local Agencies, Chapter 1, Part 1, Division 2, Title 5, commencing at Section 53130;

   (e) Title 42 United State Code (USC), Sections 300x-21 through 300x-31, 300x-34, 300x-53, 300x-57, and 330x-65 and 66;

   (f) The Single Audit Act Amendments of 1996 (Title 31, USC Sections 7501-7507) and the Office of Management and Budget (OMB) Circular A-133 revised June 27, 2003 and June 26, 2007.

   (g) Title 45, Code of Federal Regulations (CFR), Sections 96.30 through 96.33 and Sections 96.120 through 96.137;

   (h) Title 42, CFR, Sections 8.1 through 8.6~~3~~4;

   (i) Title 21, CFR, Sections 1301.01 through 1301.93, Department of Justice, Controlled Substances; and,

   (j) State Administrative Manual (SAM), Chapter 7200 (General Outline of Procedures).

   Contractor shall be familiar with the above laws, regulations, and guidelines and shall assure that its Subcontractors are also familiar with such requirements.

2. The provisions of this Exhibit A, Attachment I ~~A1~~, Part IV, are not intended to abrogate any provisions of law or regulation, or any standards existing or enacted during the term of this Contract.

3. Contractor shall adhere to the applicable provisions of Title 45, CFR, Part 96, Subparts C and L, as applicable, in the expenditure of the SAPTBG funds.

Document 1A, 45 CFR 96, Subparts C and L, is incorporated by reference.

4. Documents 1C ~~and 1D(b)~~, incorporated by this reference, contains additional requirements that shall be adhered to by those Contractors that receive these ~~types of funds specified by each document~~. These exhibits and documents ~~are~~ **is**:

   (a) Document 1C, Driving-Under-the-Influence Program Requirements;

   (b) ~~Document 1D(b), SAPT Female Offender Treatment Project (FOTP).~~

5. In accordance with the Fiscal Year 2011-12 State Budget Act and accompanying law (Chapter 40, Statues of 2011 and Chapter 13, Statues of 2011, First Extraordinary Session), contractors that provide Women and Children's Residential Treatment Services shall comply with the program requirements (Section 2.5, Required Supplemental/Recovery Support Services) of the Substance Abuse and Mental Health Services Administration's Grant Program for Residential Treatment for Pregnant and Postpartum Women, RFA found at http://www.samhsa.gov/grants/grant-announcements/ti-14-005

Section 3 - Performance Provisions

A. Monitoring

1. Contractor's performance under this Exhibit A, Attachment I ~~A2~~, Part IV, shall be monitored by the State during the term of this Contract. Monitoring criteria shall include, but not be limited to:

   (a) Whether the quantity of work or services being performed conforms to Exhibit B ~~A2~~;

   (b) Whether the Contractor has established and is monitoring appropriate quality standards;

   (c) Whether the Contractor is abiding by all the terms and requirements of this Contract;

   (d) Whether the Contractor is abiding by the terms of the Perinatal Services Network Guidelines (Document 1G); and

   (e) Contractor shall conduct annual onsite monitoring reviews of services and subcontracted services for programmatic and fiscal requirements. Contractor shall submit copy of their monitoring and audit reports to DHCS within two weeks of issuance. Reports should be sent by secure, encrypted e-mail to:

   SUDCountyReports@dhcs.ca.gov or

Substance Use Disorder - Prevention, Treatment and Recovery Services
Division, Performance Management Branch
Department of Health Care Services
PO Box 997413, MS-2627
Sacramento, CA 95899-7413;

2. Failure to comply with the above provisions shall constitute grounds for the State to suspend or recover payments, subject to the Contractor's right of appeal, or may result in termination of the Contract or both.

B. Performance Requirements

1. Contractor shall provide services based on funding set forth in Exhibit B, Attachment I ~~A2~~, and under the terms of this Contract.

2. Contractor shall provide services to all eligible persons in accordance with federal and state statutes and regulations. Contractor shall assure that in planning for the provision of services, the following barriers to services are considered and addressed:

   (a) Lack of educational materials or other resources for the provision of services;

   (b) Geographic isolation and transportation needs of persons seeking services or remoteness of services;

   (c) Institutional, cultural, and/or ethnicity barriers;

   (d) Language differences;

   (e) Lack of service advocates;

   (f) Failure to survey or otherwise identify the barriers to service accessibility; and,

   (g) Needs of persons with a disability.

3. Contractor shall comply with any additional requirements of the documents that have been incorporated herein by reference, including, but not limited to, those on the "List of Exhibit A, Attachment I ~~A1~~ Documents incorporate by Reference for Fiscal Year ~~2015-16~~ **2016-17**" which is attached to Exhibit A, Attachment I ~~A1~~.

4. Amounts awarded pursuant to Exhibit A, Attachment I ~~A1~~ shall be used exclusively for providing alcohol and/or drug program services consistent with the purpose of the funding.

5. DHCS shall issue a report to Contractor after conducting monitoring, utilization, or auditing reviews of county or county subcontracted providers. When the DHCS report identifies non-compliant services or processes, it shall require a CAP. The

Contractor, or in coordination with its subcontracted provider, shall submit a CAP to DHCS within the designated timeframe specified by DHCS.

Substance Use Disorder - Prevention, Treatment and Recovery Services Division,
Performance Management Branch
Department of Health Care Services
PO Box 997413, MS-2621
Sacramento, CA 95899-7413;

Or by secure, encrypted email to: SUDCountyReports@dhcs.ca.gov

6. The CAP shall include a statement of the problem and the goal of the actions the Contractor and/or its subcontracted provider will take to correct the deficiency or non-compliance. The CAP shall:

   (a) Address the specific actions to correct deficiency or non-compliance

   (b) Identify who/which unit(s) will act; who/which unit(s) are accountable for acting; and

   (c) Provide a timeline to complete the actions.

Exhibit A, Attachment I A2
Program Specifications

Part V: Drug Medi-Cal Treatment Program Substance Use Disorder Services

Section 1: Formation and Purpose

A. This Exhibit A, Attachment I A1, Part V of the Contract is entered into by and between the State and the Contractor for the purpose of identifying and providing for covered DMC services for substance use disorder treatment in the Contractor's service area pursuant to Sections 11848.5(a) and (b) of the Health and Safety Code (hereinafter referred to as HSC), Sections ~~14124.20,~~ 14021.51 – 14021.53, and 14124.20 – 14124.25 of the W&I **Code** , and Title 22 of the California Code of Regulations (hereinafter referred to as Title 22), Sections 51341.1, 51490.1, and 51516.1.

B. It is further agreed this Contract is controlled by applicable provisions of: (a) the W&I **Code**, Chapter 7, Sections 14000, et seq., in particular, but not limited to, Sections 14100.2, 14021, 14021.5, 14021.6, 14043, et seq., (b) Title 22, including but not limited to Sections 51490.1, 51341.1 and 51516.1; and (c) Division 4 of Title 9 of the California Code of Regulations (hereinafter referred to as Title 9).

C. It is understood and agreed that nothing contained in this contract shall be construed to impair the single state agency authority of DHCS.

D. The objective of this contract is to make substance use disorder treatment services available to Medi-Cal beneficiaries through utilization of federal and state funds available pursuant to Title XIX or Title XXI of the Social Security Act for reimbursable covered services rendered by certified DMC providers.

E. Awards under the Medical Assistance Program (CFDA 93.778) are no longer excluded from coverage under the HHS implementation of the A-102 Common Rule, 45 CFR part 92 (*Federal Register*, September 8, 2003, 68 FR 52843-52844). This change is effective for any grant award under this program made after issuance of the initial awards for the second quarter of Federal Fiscal Year 2004. This program also is subject to the requirements of 45 CFR part 95 and the cost principles under Office of Management and Budget Circular A-87 (as provided in *Cost Principles and Procedures for Developing Cost Allocation Plans and Indirect Cost Rates for Agreements with the Federal Government*, HHS Publication ASMB C-10, available on the Internet at http://www.dol.gov/oasam/boc/ASMB_C-10.pdf

Section 2: Covered Services

A. Covered Services

1. Contractor shall establish assessment and referral procedures and shall arrange, provide, or subcontract for covered services in the Contractor's service area. Covered services include:

(a) Outpatient drug-free treatment;

(b) Narcotic replacement therapy;

(c) Naltrexone treatment;

(d) Intensive Outpatient Treatment and,

(e) Perinatal Residential Substance Abuse Services (excluding room and board).

2. Narcotic treatment program services per W&I Code, Section 14124.22:

In addition to narcotic treatment program services, a narcotic treatment program provider who is also enrolled as a Medi-Cal provider may provide medically necessary treatment of concurrent health conditions within the scope of the provider's practice, to Medi-Cal beneficiaries who are not enrolled in managed care plans. Medi-Cal beneficiaries enrolled in managed care plans shall be referred to those plans for receipt of medically necessary medical treatment of concurrent health conditions.

Diagnosis and treatment of concurrent health conditions of Medi-Cal beneficiaries not enrolled in managed care plans by a narcotic treatment program provider may be provided within the Medi-Cal coverage limits. When the services are not part of the substance use disorder treatment reimbursed pursuant to **W&I Code,** Section 14021.51, services shall be reimbursed in accordance with the Medi-Cal program. Services reimbursable under this section shall include, but not limited to, all of the following:

(a) Medical treatment visits

(b) Diagnostic blood, urine, and X-rays

(c) Psychological and psychiatric tests and services

(d) Quantitative blood and urine toxicology assays

(e) Medical supplies

A narcotic treatment provider, who is enrolled as a Medi-Cal fee-for-service provider, shall not seek reimbursement from a beneficiary for substance abuse treatment services, if services for treatment of concurrent health conditions are billed to the Medi-Cal fee-for-service program.

3. In the event of a conflict between the definition of services contained in this Section of the Contract, and the definition of services in Title 22, Sections 51341.1, 51490.1, and 51516.1, the provisions of Title 22 shall govern.

4. Contractor, to the extent applicable, shall comply with "Sobky v. Smoley" (Document 2A), 855 F. Supp. 1123 (E.D. Cal 1994), incorporated by this reference.

5. Contractor shall comply with federal and state mandates to provide alcohol and other drug treatment services deemed medically necessary for Medi-Cal eligible: (1) pregnant and postpartum women, and (2) youth under age 21 who are eligible under the EPSDT Program

   (a) If Drug Medi-Cal services are provided to Minor Consent beneficiaries, Contractor shall comply with California Family Code Section 6929, and California Code of Regulations, Title 22, Sections 50147.1, 50030, 50063.5, 50157(f)(3), 50167(a)(6)(D), and 50195(d).

B. Access to Services

1. Subject to DHCS provider enrollment certification requirements, Contractor shall maintain continuous availability and accessibility of covered services and facilities, service sites, and personnel to provide the covered services through use of DMC-certified providers. Such services shall not be limited due to budgetary constraints.

   (a) When a request for covered services is made by a beneficiary, Contractor shall require services to be initiated with reasonable promptness. Contractor shall have a documented system for monitoring and evaluating accessibility of care, including a system for addressing problems that develop regarding waiting times and appointments.

   (b) The contractor shall authorize residential services in accordance with the medical necessity criteria specified in Title 22, Section 51303 and the coverage provisions of the approved state Medi-Cal Plan. Room and board are not reimbursable DMC services. If services are denied, the provider shall inform the beneficiary in accordance with Title 22, Section 51341.1 (p).

   (c) Contractor shall require that treatment programs are accessible to people with disabilities in accordance with Title 45, Code of Federal Regulations (hereinafter referred to as CFR), Part 84 and the Americans with Disabilities Act.

2. Covered services, whether provided directly by the Contractor or through Subcontractors with DMC certified and enrolled programs, shall be provided to beneficiaries without regard to the beneficiaries' county of residence.

3. The failure of the Contractor or its Subcontractors to comply with Section B of this Part will be deemed a breach of this Contract sufficient to terminate this Contract for cause. In the event the Contract is terminated, the provision of this Exhibit A, Attachment I, Part I, Section B, shall apply.

C. Payment For Services

1. The Department shall make the appropriate payments set forth in Exhibit B ~~A1~~ and take all available steps to secure and pay FFP and State General Funds (SGF) to the Contractor, once the Department receives FFP and SGF, 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.

2. Contractor shall amend its subcontracts for covered services in order to provide sufficient funds to match allowable federal Medicaid reimbursements for any increase in provider DMC services to beneficiaries.

3. In the event that the Contractor fails to provide covered services in accordance with the provisions of this Contract, at the discretion of the State, Contractor may be required to forfeit its county realignment funds pursuant to Government Code Section 30027.10 (a) through (d) from the Behavioral Health Subaccount that is set aside for Drug Medi-Cal services and surrender its authority to function as the administrator of covered services in its service area.

Section 3: Drug Medi-Cal Certification and Continued Certification

A. DMC Certification and Enrollment

1. The State will certify eligible providers to participate in the DMC program.

2. The Department shall certify any county operated or non-governmental providers. This certification shall be performed prior to the date on which the Contractor begins to deliver services under this contract at these sites.

3. Contractor shall require that providers of perinatal DMC services are properly certified to provide these services and comply with the requirements contained in Title 22, Section 51341.1, Services for Pregnant and Postpartum Women.

4. Contractor shall require all the subcontracted providers of services to be licensed, registered, DMC certified and/or approved in accordance with applicable laws and regulations. Contractor's subcontracts shall require that providers comply with the following regulations and guidelines:

   (a) Title 21, CFR Part 1300, et seq., Title 42, CFR, Part 8;

(b) Drug Medi-Cal Certification Standards for Substance Abuse Clinics (Document 2E);

(c) Title 22, CCR, Sections 51341.1, 51490.1, and 51516.1, (Document 2C);

(d) Standards for Drug Treatment Programs (October 21, 1981) (Document 2F);

(e) Title 9, CCR, Division 4, Chapter 4, Subchapter 1, Sections 10000, et seq; and

(f) Title 22, CCR, **Division 3, Chapter 3,** sections 51000 et. seq.

In the event of conflicts, the provisions of Title 22 shall control if they are more stringent.

5. The Contractor shall notify ~~the State~~ **Provider Enrollment Division (PED)** of an addition or change of information in a Providers pending DMC certification application within 35 days of receiving notification from the Provider. The Contractor must ensure that a new DMC certification application is submitted to ~~the State~~ **PED** reflecting the change.

6. The Contractor is responsible for ensuring that any reduction of covered services or relocations by providers are not implemented until approval is issued by the State. Within 35 days of receiving notification of a provider's intent to reduce covered services or relocate, the Contractor shall submit, or require the provider to submit, a DMC certification application to ~~the State~~ **PED**. The DMC certification application must be submitted to ~~the State~~ **PED** 60 days prior to the desired effective date of the reduction of covered services or relocation.

7. If, at any time, a Subcontractor's license, registration, certification, or approval to operate a substance use treatment program or provide a covered service is revoked, suspended, modified, or not renewed outside of DHCS, the Contractor must notify DHCS **Fiscal Management & Accountability Branch by e-mail at DHCSMPF@dhcs.ca.gov** within two business days of knowledge of Section 3(A(7)) of Exhibit A, Attachment ~~I A1~~.

(a) A provider's certification to participate in the DMC program shall automatically terminate in the event that the provider or its owners, officers or directors are convicted of Medi-Cal fraud, abuse or malfeasance. For purposes of this section, a conviction shall include a plea of guilty or nolo contendere.

B. Continued Certification

1. All DMC certified providers shall be subject to continuing certification requirements at least once every five years.

2. 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, the certification remains valid, and has all required fire clearances.

3. State will conduct recertification on-site visits at clinics for circumstances identified in the "Drug Medi-Cal Certification Standards for Substance Abuse Clinics" (Document 2E). Document 2E contains the appeal process in the event the State disapproves a provider's request for certification or recertification and shall be included in the Contractor's subcontracts.

Section 4: Monitoring

A. State Monitoring

1. DHCS Monitoring Reviews and Financial Audits of Contractor

The Department shall monitor the Contractor's operations for compliance with the provisions of this contract, and applicable federal and state law and regulations. Such monitoring activities shall include, but not be limited to, inspection and auditing of Contractor services, management systems and procedures, and books and records, as the Department deems appropriate, at any time during the Contractor's or facility's normal business hours. When monitoring activities identify areas of non-compliance, the Department shall issue reports to the Contractor detailing findings, recommendations, and corrective action.

2. ~~Post Service Post Payment~~ **Postservice Postpayment** Utilization Reviews

(a) After the DMC services have been rendered and paid, the Department shall conduct ~~Post Service Post Payment~~ **Postservice Postpayment (PSPP)** Utilization Reviews of the subcontracted DMC providers to determine whether the DMC services were provided in accordance with Title 22, Section 51341.1. The DHCS shall issue the PSPP report to the Contractor with a copy to subcontracted DMC provider. The Contractor shall be responsible for their subcontracted providers and their county-run programs to ensure any deficiencies are remediated pursuant to Sections 1 and 2 herein. The Contractor shall attest the deficiencies have been remediated and are complete, pursuant to Section 4(A), Paragraph (c), herein.

(b) State shall take appropriate steps in accordance with Title 22, CCR, Section 51341.1 to recover payments made if subsequent investigation uncovers evidence that the claim(s) should not have been paid or that DMC services have been improperly utilized, and/or shall take the corrective action as appropriate. If programmatic or fiscal deficiencies are identified, the Provider shall be required to submit a Corrective Action Plan (CAP) to ~~DHCS via the Contractor for approval~~ **the Contractor for review and approval prior to submission to DHCS for final approval.**

i. Pursuant to CCR, Title 22, Section 51341.1(o), all deficiencies identified by the PSPP review, whether or not a recovery of funds results, must be corrected and the entity that provided the services must submit a **Contractor-approved** CAP to the ~~DMC~~ PSPP Unit within 60 days of the date of the PSPP report.

1. The plan shall:

a. Address each demand for recovery of payment and/or programmatic deficiency;

b. Provide a specific description of how the deficiency shall be corrected; and

c. Specify the date of implementation of the corrective action.

d. Identify who will be responsible for correction and who will be responsible for on-going compliance.

2. DHCS will provide written approval of the CAP to the Contractor with a copy to the Provider. If DHCS does not approve the CAP, DHCS will provide guidance on the deficient areas and request an updated CAP from the Contractor with a copy to the Provider. The entity that provided the services must submit an updated CAP to the DMC PSPP Unit within 30 days of notification.

3. If the entity that provided the services, does not submit a CAP, or, does not implement the approved CAP provisions within the designated timeline, then DHCS may withhold funds from the Contractor until the ~~the~~ entity that provided the services is in compliance with Exhibit A, Attachment I ~~A1~~, Part V, Section 4(A)(2). The State shall inform the Contractor when funds will be withheld.

(c) Contractor and/or Subcontractor may appeal DMC dispositions concerning demands for recovery of payment and/or programmatic deficiencies of specific claims. Such appeals shall be handled pursuant to Title 22, CCR, Section 51341.1(q). This section shall not apply to those grievances or complaints arising from the financial findings of an audit or examination made by or on behalf of the State pursuant to Exhibit B ~~A1~~, Part II, Section 3, of this Contract.

(d) State shall monitor the Subcontractor's compliance with PSPP utilization review requirements in accordance with Title 22. Counties are also required to monitor of the Subcontractor's compliance pursuant to Section 4, Paragraph A.2, of this contract. The federal government may also review the existence and effectiveness of the State's utilization review system.

(e) Contractor shall implement and maintain compliance with the system of review described in Title 22, Section 51341.1, for the purposes of reviewing the utilization, quality, and appropriateness of covered services and ensuring that all applicable Medi-Cal requirements are met.

(f) Contractor shall assure that Subcontractor sites must keep a record of the clients/patients being treated at that location. Contractor shall retain client records for a minimum of three (3) years from the date of the last face-to-face contact. When an audit by the Federal Government or the State has been started before the expiration of the three-year period, the client records shall be maintained until completion of the audit and the final resolution of all issues as a result of the audit.

3. Training

(a) DHCS's Substance Use Disorder - Prevention, Treatment, and Recovery Services Division (SUD PTRSD) shall provide mandatory annual training to the Contractor on the requirements of Title 22 and the Drug Medi-Cal program requirements.

(b) Contractor may request additional Technical Assistance or training from SUD PTRSD on an ad hoc basis.

B. Contractor Monitoring

1. Program Integrity: Contractor is responsible for ensuring program integrity of its services and its subcontracted providers through a system of oversight, which shall include at least the following:

(a) Compliance with state and federal law and regulations, including, but not limited to, 42 CFR 433.32, 42 CFR 433.51, 42 CFR 431.800 et. seq., 42 CFR 440.230, 42 CFR 440.260, 42 CFR 455 et. seq., 42 CFR 456 et. seq., 42 CFR 456.23, 22 CCR 51490, 22 CCR 51490.1, 22 CCR 51341.1, 22 CCR 51159, WIC 14124.1, WIC 14124.2, 42 CFR 438.240(e), 42 CFR 438.240(b)(3), 42 CFR 438.240, 42 CFR 438.416, 42 CFR 438-10, and 42 CFR 438.206.

(b) Contractor shall conduct, at least annually, ~~an audit~~ **a utilization review** of DMC providers to assure covered services are being appropriately rendered. The annual ~~audit~~ **review** must include an on-site visit of the service provider. Reports of the annual ~~audit~~ **review** shall be provided to the Department's Performance Management Branch at:

Substance Use Disorder - Prevention, Treatment and Recovery Services
Division, Performance Management Branch
Department of Health Care Services
PO Box 997413, MS-2621
Sacramento, CA 95899-7413;

Or by secure, encrypted email to: SUDCountyReports@dhcs.ca.gov

~~Audit~~ **Review** reports shall be provided to the State within 2 weeks of completion by the Contractor.

Technical assistance is available to counties from DHCS SUD PTRSD.

(c) Contractor shall ensure that DATAR submissions, detailed in Part III, Paragraph G of this contract are complied with by all treatment providers and subcontracted treatment providers. Contractor shall attest that each subcontracted provider is enrolled in DATAR at the time of execution of the subcontract.

(d) Contractor must monitor and attest compliance and/or completion by Providers with CAP requirements (detailed in Section 4, Paragraph (A)(2)(c)) **of this Exhibit** as required by any PSPP review. Contractor shall attest to DHCS, using the form developed by DHCS that the requirements in the CAP have been completed by the Contractor and/or the Provider. Submission of DHCS Form 8049 by Contractor must be accomplished within the timeline specified in the approved CAP, as noticed by DHCS.

(e) Contractor shall attest that DMC claims submitted to the state have been subject to review and verification process for accuracy and legitimacy. (45 CFR 430.30, 433.32, 433.51). Contractor shall not knowingly submit claims for services rendered to any beneficiary after the beneficiary's date of death, or from uncertified or decertified providers.

2. Training to DMC Subcontractors

(a) Contractor shall ~~provide~~ **ensure that all Subcontractors receive** training on the requirements of Title 22 regulations and DMC requirements at least annually**.** ~~to all subcontracted providers. Attendance~~ **Documented attendance** of any subcontracted provider at the annual trainings offered by DHCS (specified in Section 4, paragraph (A) (3) of this contract) shall suffice to meet the requirements of this provision. Contractor shall report compliance with this section to DHCS annually as part of the DHCS County monitoring process.

3. Monthly Monitoring

(a) Contractor shall check the status of all providers monthly to ensure that they are continuing active participation in the DMC program. Any subcontracted provider who surrenders their certification or closes their facility must be reported by the Contractor to ~~the Department~~ **DHCS' County Monitoring Unit** within two (2) business days of notification or discovery.

(b) During the monthly status check, the Contractor shall monitor for a triggering recertification event (change in ownership, change in scope of services, remodeling of facility, or change in location) and report any triggering events to ~~the State~~ **DHCS' County Monitoring Unit** within two (2) business days of notification or discovery.

4. Program Complaints

(a) All complaints received by Contractor regarding a DMC certified facility shall be forwarded to:

Drug Medi-Cal Complaints are to be submitted to:

Department of Heath Care Services
P.O. Box 997413
Sacramento, CA 95899-7413
Call the Hotline
Phone Toll-Free: (800) 822-6222
~~Division Chief~~
~~Substance Use Disorders Prevention, Treatment and Recovery Services Division~~
~~Department of Health Care Services~~
~~P.O. Box 997413, MS# 2621~~
~~Sacramento, CA 95899-7413~~

Complaints for Residential Adult Alcoholism or Drug Abuse Recovery or Treatment Facilities may also be made by telephoning the appropriate licensing branch listed below:

SUD Compliance Division:

Public Number: (916) 322-2911
Toll Free Number: (877) 685-8333

The Complaint Form is available and can also be submitted online at:
http://www.dhcs.ca.gov/individuals/Pages/Sud-Complaints.aspx

(b) Counties shall be responsible for investigating complaints and providing the results of all investigations to the Department e-mail address by secure, encrypted e-mail to: SUDCountyReports@dhcs.ca.gov within two (2) business days of completion.

5. Record Retention

(a) Contractor shall include instructions on record retention and include in any subcontract with providers the mandate to keep and maintain records for each service rendered, to whom it was rendered, and the date of service, pursuant to W&I **Code,** Section 14214.1 and 42 CFR 433.32; and 22 CCR section 51341.1.

6. Subcontract Termination

(a) The Contractor must notify ~~DHCS~~ **DHCS' County Monitoring Unit** of the termination of any contract with a certified subcontracted provider, and the basis for termination of the contract, within two (2) business days.

7. Corrective Action Plan

(a) If the Contractor fails to ensure any of the foregoing oversight through an adequate system of monitoring, utilization review, and fiscal and programmatic controls, the Department may request a CAP from the Contractor to address these deficiencies and a timeline for implementation. Failure to submit a CAP or adhere to the provisions in the CAP can result in a withhold of SAPT funds allocated to Contractor for the provision of services, and/or termination of this contract for cause

(b) Failure to comply with Monitoring requirements shall result in:

i. DHCS shall issue a report to Contractor after conducting monitoring, utilization, or fiscal auditing reviews of a county. When the DHCS report identifies non-compliant services or processes, it shall require a CAP. The Contractor shall submit a CAP to DHCS within the ~~following~~ timeframes ~~of receipt of the~~ **required by** DHCS ~~report~~.

a. The CAP shall include**:** ~~a statement of the problem and the goal of the actions the Contractor or its subcontracted provider will take to correct the deficiency or non-compliance. The CAP shall:~~

(1) **A statement of the deficiency;**
~~Address the specific actions to correct deficiency or non-compliance;~~

~~Identify who/which unit(s) will act; who/which unit(s) are accountable for acting; and~~

(2) **A list of action steps to be taken to correct the deficiency;** ~~Provide a timeline to complete the actions~~.

(3) **Date of completion of each deficiency corrected;**

(4) **Who will be responsible for correction and ongoing compliance.**

ii. DHCS will provide written approval of the CAP to the Contractor ~~and the subcontracted provider~~. If DHCS does not approve the CAP submitted by the Contractor, DHCS will provide guidance on the deficient areas and request an updated CAP from the Contractor with a new deadline for submission.

iii. If the Contractor does not submit a CAP, or, does not implement the approved CAP provisions within the designated timeline, then the State may withhold funds until the Contractor is in compliance. The State shall inform the Contractor when funds will be withheld.

Section 5: Investigations and Confidentiality of Administrative Actions

A. Contractor acknowledges that if a DMC provider is under investigation by the State or any other state, local or federal law enforcement agency for fraud or abuse, the State may temporarily suspend the provider from the DMC program, pursuant to W&I **Code,** Section 14043.36(a). Information about a provider's administrative sanction status is confidential until such time as the action is either completed or resolved. The DHCS may also issue a Payment Suspension to a provider pursuant to W&I **Code,** Section 14107.11 and Code of Federal Regulations, Title 42, section 455.23. The Contractor is to withhold payments from a DMC provider during the time a Payment Suspension is in effect.

B. Contractor shall execute the Confidentiality Agreement, attached as Document 5A. The Confidentiality Agreement permits DHCS to communicate with Contractor concerning subcontracted providers that are subject to administrative sanctions.

EXHIBIT A, ATTACHMENT I A2

DOCUMENTS INCORPORATED BY REFERENCE

The following documents are hereby incorporated by reference into the County contract though they may not be physically attached to the contract but will be issued in a CD under separate cover:

Document 1A:	Title 45, Code of Federal Regulations 96, Subparts C and L, Substance Abuse Prevention and Treatment Block Grant Requirements https://www.gpo.gov/fdsys/granule/CFR-2005-title45-vol1/CFR-2005-title45-vol1-part96 ~~http://www.access.gpo.gov//nara/cfr/waisidx_04/45cfr96_04.html~~
Document 1B:	Title 42, Code of Federal Regulations, Charitable Choice Regulations https://www.law.cornell.edu/cfr/text/42/part-54 ~~http://www.access.gpo.gov//nara/cfr/waisidx_04/42cfr54_04.html~~
Document 1C:	Driving-Under-the-Influence Program Requirements
~~Document 1D(b):~~	~~SAPT Female Offender Treatment Project (FOTP)~~
Document 1F(a):	Reporting Requirement Matrix – County Submission Requirements for the Department of Health Care Services
Document 1G:	Perinatal Services Network Guidelines ~~2014~~ **2015** ~~(for Non-DMC Perinatal Programs)~~
Document 1H(a):	Service Code Descriptions
Document 1H(b):	Program Code Listing
Document 1H(c) :	Funding Line Descriptions
Document 1J(a):	Non-Drug Medi-Cal Audit Appeals Process
Document 1J(b):	DMC Audit Appeals Process
Document 1K:	Drug and Alcohol Treatment Access Report (DATAR) http://www.dhcs.ca.gov/provgovpart/Pages/DATAR.aspx
Document 1P:	Alcohol and/or Other Drug Program Certification Standards (March 15, 2004) http://www.dhcs.ca.gov/provgovpart/Pages/Facility_Certification.aspx

Document 1T:	CalOMS Prevention Data Quality Standards
Document 1V:	Youth Treatment Guidelines http://www.dhcs.ca.gov/individuals/Documents/Youth_Treatment_Guidelines.pdf
Document 2A:	Sobky v. Smoley, Judgment, Signed February 1, 1995
Document 2C:	Title 22, California Code of Regulations http://ccr.oal.ca.gov
Document 2E:	Drug Medi-Cal Certification Standards for Substance Abuse Clinics (Updated July 1, 2004) http://www.dhcs.ca.gov/services/adp/Documents/DMCA_Drug_Medi-Cal_Certification_Standards.pdf
Document 2F:	Standards for Drug Treatment Programs (October 21, 1981) http://www.dhcs.ca.gov/services/adp/Documents/DMCA_Standards_for_Drug_Treatment_Programs.pdf
Document 2K:	Multiple Billing Override Certification (MC 6700)
Document 2L(a):	Good Cause Certification (~~MC~~ 6065A)
Document 2L(b):	Good Cause Certification (~~MC~~ 6065B)
Document 2P:	County Certification - Cost Report Year-End Claim For Reimbursement
Document 2P(a):	Drug Medi-Cal Cost Report Forms – Intensive Outpatient Treatment – Non-Perinatal (form and instructions)
Document 2P(b):	Drug Medi-Cal Cost Report Forms – Intensive Outpatient Treatment – Perinatal (form and instructions)
Document 2P(c):	Drug Medi-Cal Cost Report Forms – Outpatient Drug Free Individual Counseling – Non-Perinatal (form and instructions)
Document 2P(d):	Drug Medi-Cal Cost Report Forms – Outpatient Drug Free Individual Counseling – Perinatal (form and instructions)
Document 2P(e):	Drug Medi-Cal Cost Report Forms – Outpatient Drug Free Group Counseling – Non-Perinatal (form and instructions)
Document 2P(f):	Drug Medi-Cal Cost Report Forms – Outpatient Drug Free Group Counseling

	– Perinatal (form and instructions)
Document 2P(g):	Drug Medi-Cal Cost Report Forms – Residential – Perinatal (form and instructions)
Document 2P(h):	Drug Medi-Cal Cost Report Forms – Narcotic Treatment Program – County – Non-Perinatal (form and instructions)
Document 2P(i):	Drug Medi-Cal Cost Report Forms – Narcotic Treatment Program – County – Perinatal (form and instructions)
Document 3G:	California Code of Regulations, Title 9 – Rehabilitation and Developmental Services, Division 4 – Department of Alcohol and Drug Programs, Chapter 4 – Narcotic Treatment Programs http://www.calregs.com
Document 3H:	California Code of Regulations, Title 9 – Rehabilitation and Developmental Services, Division 4 – Department of Alcohol and Drug Programs, Chapter 8 – Certification of Alcohol and Other Drug Counselors http://www.calregs.com
Document 3J:	CalOMS Treatment Data Collection Guide http://www.dhcs.ca.gov/provgovpart/Documents/CalOMS_Tx_Data_Collection_Guide_JAN%202014.pdf
Document 3O:	Quarterly Federal Financial Management Report (QFFMR) 2014-15 http://www.dhcs.ca.gov/provgovpart/Pages/SUD_Forms.aspx
Document 3S	CalOMS Treatment Data Compliance Standards
Document 3T	Non-Drug Medi-Cal and Drug Medi-Cal Local Assistance Funding Matrix
Document 3T(a)	SAPT Authorized and Restricted Expenditures Information (Nov 2012)
Document 3V	Culturally and Linguistically Appropriate Services (CLAS) National Standards http://minorityhealth.hhs.gov/templates/browse.aspx?lvl=2&lvlID=15
Document 4A :	Drug Medi-Cal Claim Submission Certification – County Contracted Provider – DHCS Form MC 8186 with Instructions
Document 4B :	Drug Medi-Cal Claim Submission Certification – County Operated Provider – DHCS Form MC 8187 with Instructions
Document 4D :	Drug Medi-Cal Certification for Federal Reimbursement (DHCS 100224A)

Document 4E :	Treatment Standards for Substance Use Diagnosis: A Guide for Services (Spring 2010)
Document 4F :	Drug Medi-Cal (DMC) Services Quarterly Claim for Reimbursement of County Administrative Expenses (Form #MC 5312)
Document 5A :	Confidentiality Agreement

Exhibit B A2
Budget Detail and Payment Provisions

Part I – General Fiscal Provisions

Section 1 – General Fiscal Provisions

A. Fiscal Provisions

For services satisfactorily rendered, and upon receipt and approval of documentation as identified in Exhibit A, Attachment I ~~A1~~, Part III, DHCS agrees to compensate the Contractor for actual expenditures incurred in accordance with the rates and/or allowable costs specified herein.

B. Use of State **General** Funds

Contractor may not use allocated Drug Medi-Cal State General Funds to pay for any non-Drug Medi-Cal services.

C. Funding Authorization

Contractor shall bear the financial risk in providing any substance use disorder services covered by this Contract.

D. Availability of Funds

It is understood that, for the mutual benefit of both parties, this Contract may have been written before ascertaining the availability of congressional appropriation of funds in order to avoid program and fiscal delays that would occur if this Contract were not executed until after that determination. If so, State may amend the amount of funding provided for in this Contract based on the actual congressional appropriation.

E. Subcontractor Funding Limitations

Pursuant to HSC Section 11818 **(b)**(2)(A), Contractor shall reimburse its Subcontractors that receive a combination of **Drug** Medi-Cal funding and other federal or county realignment funding for the same service element and location based on the Subcontractor's actual costs in accordance with Medicaid reimbursement requirements as specified in Title XIX or Title XXI of the Social Security Act; Title 22, and the State's Medicaid Plan. Payments at negotiated rates shall be settled to actual cost at year-end.

F. Budget Contingency Clause

It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, DHCS shall have no liability to pay any funds whatsoever to Contractor or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.

If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, DHCS shall have the option to either cancel this Agreement with no liability occurring to DHCS, or offer an **amended** agreement ~~amendment~~ to Contractor to reflect the reduced amount.

G. Expense Allowability / Fiscal Documentation

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

2. Contractor shall maintain for review and audit and supply to DHCS upon request, adequate documentation of all expenses claimed pursuant to this Agreement to permit a determination of expense allowability.

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

4. Costs and/or expenses deemed unallowable are subject to recovery by DHCS.

H. Maintenance of Effort for SAPT Block Grant

1. Notwithstanding any other provision in this contract, the Director may reduce federal funding allocations, on a dollar-for-dollar basis, to a county that has a reduced or anticipates reduced expenditures in a way that would result in a decrease in ~~the~~ **California's receipt of** federal Substance Abuse Prevention and Treatment Block Grant funds (42 U.S.C. Sect 300x-30).

2. Prior to making any reductions pursuant to this subdivision, the Director shall notify all counties that county underspending will reduce the federal Substance Abuse Prevention and Treatment Block Grant maintenance of effort (MOE). Upon receipt of notification, a county may submit a revision to the county budget initially submitted pursuant to subdivision (a) of Section ~~11978~~ **11798** in an effort to maintain the statewide SAPT Block Grant MOE.

3. **Pursuant to 45 CFR 96.124 C 1-3 the Contractor shall expend a specified percentage of SAPT Block Grant funds for perinatal services, pregnant women, and women with dependent children each state fiscal year (SFY). The Contractor shall expend that percentage of SAPT Block Grant funds by, either establishing new programs or expanding the capacity of existing programs. In accordance with 45 CFR 96.124 (c)(1-3), the Contractor shall calculate the percentage of funds to be expended for perinatal services, pregnant women, and women with dependent children in the manner described in Exhibit G: County Share of SAPT Block Grant Women Services Expenditure Requirement.**

4. Pursuant to subdivision (b) of Section ~~11978.1~~ **11798.1**, a county shall notify the Department in writing of proposed local changes to the county's expenditure of funds. The Department shall review and may approve the proposed local changes depending on the level of expenditures needed to maintain the statewide SAPT Block Grant MOE.

I. Effective the date of execution of this Contract, nothing in this Contract waives the protections provided to Contractor under Section 36 of article XIII of the California Constitution ("Proposition 30"). Except where specifically stated in the terms of this contract, Contractor's performance of any additional legal requirements, including, but not limited to court-ordered requirements and statutory or regulatory amendments, is subject to Proposition 30's funding requirements.

Section 2 – General Fiscal Provisions – Non-Drug Medi-Cal

A. Revenue Collection

Contractor shall conform to revenue collection requirements in Division 10.5 of the HSC, Sections 11841, by raising revenues in addition to the funds allocated by the State. These revenues include, but are not limited to, fees for services, private contributions, grants, or other governmental funds. These revenues shall be used in support of additional alcohol and other drug services or facilities. Each alcohol and drug program shall set and collect client fees based on the client's ability to pay. The fee requirement shall not apply to prevention and early intervention services. Contractor shall identify in its annual cost report the types and amounts of revenues collected.

B. Cost Efficiencies

It is intended that the cost to the Contractor in maintaining the dedicated capacity and units of service shall be met by the non-DMC funds allocated to the Contractor and other Contractor or Subcontractor revenues. Amounts awarded pursuant to Exhibit A, Attachment I ~~A1~~, Part IV, shall not be used for services where payment has been made, or can reasonably be expected to be made under any other state or federal compensation or benefits program, or where services can be paid for from revenues.

Section 3 – General Fiscal Provisions – Drug Medi-Cal

A. Return of Unexpended Funds

Contractor assumes the total cost of providing covered services on the basis of the payments delineated in this Exhibit B ~~A1~~, Part II. Any State General Funds or federal Medicaid funds paid to the Contractor, but not expended for DMC services shall be returned to the State.

B. Amendment or Cancellation Due to Insufficient Appropriation

This Contract is valid and enforceable only if sufficient funds are made available to the State by the United States Government for the purpose of the DMC program. It is mutually agreed that if the Congress does not appropriate sufficient funds for this program, State has the option to void this contract or to amend the Contract to reflect any reduction of funds.

C. Exemptions

Exemptions to the provisions of Item B above, of this Exhibit, may be granted by the California Department of Finance provided that the Director of DHCS certifies in writing that federal funds are available for the term of the contract.

D. Allowable costs

Allowable costs, as used in Section 51516.1 of Title 22 shall be determined in accordance with Title 42, CFR Parts 405 and 413, and Centers for Medicare and Medicaid Services (CMS), "Medicare Provider Reimbursement Manual (Publication Number 15)," which can be obtained from the Centers for Medicare & Medicaid Services, or www.cms.hhs.gov." In accordance with W&IC Sections 14132.44 and 14132.47, funds allocated to the Contractor for DMC services, including funding for alcohol and other drug services for pregnant and postpartum women pursuant to Title 22, Section 51341.1(c), may not be used as match for targeted case management services or for Medi-Cal administrative activities.

Exhibit B A2
Budget Detail and Payment Provisions

Part II – Reimbursements

Section 1. General Reimbursement

A. Prompt Payment Clause

Payment will be made in accordance with, and within the time specified in, Government Code Chapter 4.5, commencing with Section 927.

B. Amounts Payable

1. The amount payable under this Agreement shall not exceed the amount identified on the Standard Agreement.

2. Reimbursement shall be made for allowable expenses up to the amount annually encumbered commensurate with the state fiscal year in which services are performed and/or goods are received.

3. The funds identified for the fiscal years covered by under this Section, within this Exhibit, are subject to change depending on the availability and amount of funds appropriated by the Legislature and the Federal Government. The amount of funds available for expenditure by the Contractor shall be limited to the amount identified in the final allocations issued by the State for that fiscal year or the non-DMC amount, whichever is less. Changes to allocated funds will require written amendment to the Contract.

4. For each fiscal year, the State may settle costs for services based on each fiscal year year-end cost settlement report as the final amendment for the specific fiscal year cost settlement report to the approved single state/county contract.

Section 2. Non-Drug Medi-Cal

A. Amounts Payable for Non-Drug Medi-Cal

1. State shall reimburse the Contractor monthly in arrears an amount equal to one-twelfth of the maximum amount allowed pursuant to Exhibit B ~~A1~~ of the contract or the most recent allocation based on the Budget Act Allocation, whichever is less. Final allocations will reflect any increases or reductions in the appropriations as reflected in the State Budget Act allocation and any subsequent allocation revisions.

2. Monthly disbursement to the Contract at the beginning of each fiscal year of the Contract shall be based on the preliminary allocation of funds, as detailed in this Exhibit.

3. However, based on the expenditure information submitted by the counties in the Quarterly Federal Financial Management Report (QFFMR) (Document 3O), State

may adjust monthly payments of encumbered block grant federal funds to extend the length of time (not to exceed 21 months) over which payments of federal funds will be made.

4. Monthly disbursements to the Contractor at the beginning of each fiscal year of the Contract shall be based on the preliminary allocation of funds, as detailed in Exhibit B ~~A1~~.

5. State may withhold monthly non-DMC payments if the Contractor fails to:

   (a) ~~timely~~ submit **timely** reports and data required by the State, including but not limited to, reports required pursuant to Exhibit A, Attachment I ~~A1~~, Part III.

   (b) submit the contract amendment within 90 days from issuance from the State to the Contractor.

   (c) submit and attest the completion of Corrective Action Plans for services provided pursuant to this contract.

6. Upon the State's receipt of the complete and accurate reports, data, or signed contract, the Contractor's monthly payment shall commence with the next scheduled monthly payment, and shall include any funds withheld due to late submission of reports, data and/or signed contract.

7. Adjustments may be made to the total of the Contract and amounts may be withheld from payments otherwise due to the Contractor hereunder, for nonperformance to the extent that nonperformance involves fraud, abuse, or failure to achieve the objectives of the provisions of Exhibit A, Attachment I ~~A1~~, Part IV.

B. Payment Provisions

For each fiscal year, the total amount payable by the State to the Contractor for services provided under Exhibit A, Attachment I ~~A1~~, Part IV, shall not exceed the encumbered amount. The funds identified for the fiscal years covered by Exhibit A, Attachment I ~~A1~~, Part IV, are subject to change depending on the availability and amount of funds appropriated by the Legislature and the Federal Government. Changes to encumbered funds will require written amendment to the Contract. State may settle costs for non-DMC services based on the year-end cost settlement report as the final amendment to the approved single state/county contract.

C. In the event **of** a contract amendment**,** ~~is~~ **as** required ~~pursuant to~~ **by** the preceding paragraph, Contactor shall submit to the State information as identified in Exhibit E, Section 1.D. To the extent the Contractor is notified of the State Budget Act allocation prior to the execution of the Contract, the State and the Contractor may agree to amend the contract after the issuance of the first ~~revised~~ **Budget Act** allocation.

D. Accrual of Interest

Any interest accrued from State-allocated funds and retained by the Contractor must be used for the same purpose as the State allocated funds from which the interest was accrued.

E. Expenditure Period

Substance Abuse Prevention and Treatment (SAPT) Block Grant funds are allocated based upon the Federal Grant award period. These funds must be expended for activities authorized pursuant to 42 USC Sections 300x-21(b) through 300x-66; and Title 45, CFR, Subpart L, within the availability period of the grant award. Any SAPT Block Grant funds that have not been expended by a Contractor at the end of the expenditure period identified below shall be returned to the State for subsequent return to the Federal government.

1. The expenditure period of the FFY 2014 award is October 1, 2013 through June 30, 2015.

2. The expenditure period of the FFY 2015 award is October 1, 2014 through June 30, 2016.

3. The expenditure period of the FFY 2016 award is October 1, 2015 through June 30, 2017.

4. The expenditure period of the FFY 2017 award is October 1, 2016 through June 30, 2018.

5. The expenditure period of the FFY 2018 award is October 1, 2017 through June 30, 2019.

F. Contractors receiving SAPT Block Grant funds shall comply with the financial management standards contained in Title 45, CFR, Part 92, Sections 92.20(b)(1) through (6), and Title 45, CFR, Part 96, Section 96.30.

G. Non-profit Subcontractors receiving SAPT Block Grant funds shall comply with the financial management standards contained in Title 45, CFR, Part 74, Sections 74.21(b)(1) through (4) and (b)(7), and Part 96, Section 96.30.

H. Contractors receiving SAPT Block Grant funds shall track obligations and expenditures by individual SAPT Block Grant award, including, but not limited to, obligations and expenditures for primary prevention, services to pregnant women and women with dependent children. "Obligation" shall have the same meaning as used in Title 45, CFR, Part 92, Section 92.3."

Additionally, Contractors expending SAPT Block Grant HIV Set Aside funds for HIV Early Intervention Services are required to collect data regarding their use of HIV Set-Aside funds and to report this data to the State.

I. Restrictions on the Use of ~~Federal~~ **SAPT** Block Grant Funds

Pursuant to 42 U.S.C. 300x-31, Contractor shall not use SAPT Block Grant funds provided by the Agreement on the following activities:

1. Provide inpatient services;

2. Make cash payment to intended recipients of health services;

3. Purchase or improve land, purchase, construct or permanently improve (other than minor remodeling) any building or other facility or purchase major medical equipment;

4. Satisfy any requirement for the expenditure of non-~~F~~federal funds as a condition for the receipt of ~~F~~federal funds;

5. Provide financial assistance to any entity other than a public or nonprofit private entity;

6. Pay the salary of an individual through a grant or other extramural mechanism at a rate in excess of level I of the Executive Salary Schedule for the award year: see http://grants.nih.gov/grants/policy/salcap_summary.htm;

7. Purchase treatment services ~~and~~ **in** penal or correctional institutions of this State of California; and

8. Supplant state funding of programs to prevent and treat substance abuse and related activities.

Section 3. Drug Medi-Cal

A. To the extent that the Contractor provides the covered services in a satisfactory manner and in accordance with the terms and conditions of this Contract, the State agrees to pay the Contractor federal Medicaid funds according to Exhibit A, Attachment I ~~A1~~, Part III. Subject to the availability of such funds, Contractor shall receive federal Medicaid funds and/or State General Funds for allowable expenditures as established by the federal government and approved by the State, for the cost of services rendered to beneficiaries.

B. Any payment for covered services rendered pursuant to Exhibit A, Attachment I ~~A1~~, Part V, shall only be made pursuant to applicable provisions of Title XIX or Title XXI of the Social Security Act; the W&IC; the HSC; California's Medicaid State Plan; and Sections 51341.1, 51490.1, 51516.1, and 51532 of Title 22.

C. It is understood and agreed that failure by the Contractor or its Subcontractors to comply with applicable federal and state requirements in rendering covered services shall be sufficient cause for the State to deny payments to and/or recover payments from the Contractor and/or terminate the Contractor or its Subcontractor from DMC program participation. If the State or the Department of Health and Human Services (DHHS) disallows or denies payments for any claim, Contractor shall repay to the State the federal

Medicaid funds and/or State General Funds it received for all claims so disallowed or denied. The overpayment shall be recovered by any of the methods allowed in Title 22, CCR, Sections 51047(a) and (b).

D. Before such denial, recoupment, or disallowances are made, State shall provide the Contractor with written notice of its proposed action. Such notice shall include the reason for the proposed action and shall allow the Contractor sixty (60) days to submit additional information before the proposed action is taken, as required in Title 22, CCR, Section 51047(a). This requirement does not apply to the DMC Post Service Post Payment Utilization Reviews.

E. The State shall refund to the Contractor any recovered Federal Drug Medi-Cal overpayment that is subsequently determined to have been erroneously collected, together with interest, in accordance with Title 22, CCR, Section 51047(e).

F. Contractor shall be reimbursed by the State on the basis of its actual net reimbursable cost, not to exceed the unit of service maximum rate.

G. Claims submitted to the contractor by a sub-contracted provider that is not certified or whose certification has been suspended pursuant to the Welfare and Institutions Code section 14107.11, and Code of Federal Regulations, Title 42, section 455.23 shall not be certified or processed for federal or state reimbursement by the contractor. Payments for any DMC services shall be held by the Contractor until the payment suspension is resolved.

H. In the event a contract amendment is required pursuant to the preceding paragraph, Contractor shall submit to the State information as identified in Exhibit E, Section 1.D. To the extent the Contractor is notified of the State Budget Act allocation prior to the execution of the Contract, the State and the Contractor may agree to amend the contract after the issuance of the first revised allocation.

I. Reimbursement for covered services, other than NTP services, shall be limited to the lower of:

1. the provider's usual and customary charges to the general public for the same or similar services;

2. the provider's actual allowable costs; or

3. the DMC SMA for the modality.

J. Reimbursement to NTP's shall be limited to the lower of either the USDR rate, pursuant to W&IC Section 14021.51(h), or the provider's usual and customary charge to the general public for the same or similar service. However, reimbursement paid by a county to an NTP provider for services provided to any person subject to Penal Code Sections 1210.1 or 3063.1 and for which the individual client is not liable to pay, does not constitute a usual or customary charge to the general public. (W&IC Section 14021.51(h)(2)(A)).

K. State shall reimburse the Contractor the State General Funds and/or federal Medicaid amount of the approved DMC claims and documents submitted in accordance with Exhibit A, Attachment I ~~A1~~, Part III.

L. State will adjust subsequent reimbursements to the Contractor to actual allowable costs. Actual allowable costs are defined in the Medicare Provider Reimbursement Manual (CMS-Pub.15), which can be obtained from the Centers for Medicare & Medicaid Services, Baltimore, Maryland, or www.cms.hhs.gov.

M. Contractors and Subcontractors must accept, as payment in full, the amounts paid by the State in accordance with Title 22, CCR, Section 51516.1, plus any cost sharing charges (deductible, coinsurance, or copayment) required to be paid by the client. However, Contractors and Subcontractors may not deny services to any client eligible for DMC services on account of the client's inability to pay or location of eligibility. Contractors and Subcontractors may not demand any additional payment from the State, client, or other third party payers.

Section 4. Drug Medi-Cal Direct Provider Contracts

A. Pursuant to W&IC 14124.21, DHCS shall contract with qualified DMC providers within the county when a county does not contract to operate DMC services, in whole or in part.

B. The State will invoice the Contractor for the county realignment share of approved DMC claims received by the State from the State's subcontractor. Contractor shall reimburse the State for the county realignment share of the approved DMC claims within 30 days of receipt of the invoice. If Contractor does not reimburse the State within 30 days of receipt of the invoice, the State may offset the amount owed from any other funding owed to Contractor by the State or any other State agency. The parties acknowledge that the State's subcontractor shall be responsible for repayment of any disallowed claims. However, in no event shall the State be liable for Medicaid reimbursement for any disallowed claims.

1. Any Contractor contracting with the State for the provision of services through NTP providers may receive reimbursement of the NTP administrative rate.

2. As a result of the direct contract provider's settled cost report, any County Realignment funds owed to the direct contract provider will be handled through an invoice process to the Contractor. Additionally, as a result of the direct contract provider's settled cost report, any County Realignment funds owed to the State will be returned to the Contractor.

Exhibit B A2
Budget Detail and Payment Provisions

Part III - Financial Audit Requirements

Section 1. General Fiscal Audit Requirements

A. In addition to the requirements identified below, the Contractor and its Subcontracts are required to meet the audit requirements as delineated in Exhibit C, General Terms and Conditions, and Exhibit D(F), Special Terms and Conditions, of this Contract.

B. All expenditures of county realignment funds, state and federal funds furnished to the Contractor and its Subcontractors pursuant to this Contract are subject to audit by the State. Such audits shall consider and build upon external independent audits performed pursuant to audit requirements of the Office of Management and Budget (OMB) Circular A-133 (Revised December 2013) and/or any independent Contractor audits or reviews. Objectives of such audits may include, but not limited to, the following:

1. To determine whether units of service claimed/reported are properly documented by service records and accurately accumulated for claiming/reporting;

2. To validate data reported by the Contractor for prospective contract negotiations;

3. To provide technical assistance in addressing current year activities and providing recommendation on internal controls, accounting procedures, financial records, and compliance with laws and regulations;

4. To determine the cost of services, net of related patient and participant fees, third-party payments, and other related revenues and funds;

5. To determine that expenditures are made in accordance with applicable state and federal laws and regulations and contract requirements, and/or;

6. To determine the facts in relation to analysis of data, complaints, or allegations, which may be indicative of fraud, abuse, willful misrepresentation, or failure to achieve the Contract objectives of Exhibit C and D(F).

C. Unannounced visits may be made at the discretion of the State.

D. The refusal of the Contractor or its Subcontractors to permit access to and inspection of electronic or print books and records, physical facilities, and/or refusal to permit interviews with employees, as described in this part constitutes an express and immediate material breach of this Contract and will be sufficient basis to terminate the Contract for cause or default.

E. Reports of audits conducted by the State shall reflect all findings, recommendations, adjustments and corrective action as a result of it's finding in any areas.

Section 2. Non-Drug Medi-Cal Financial Audits

A. Pursuant to OMB Circular A-133 §__.400(d)(3), Contractor shall monitor the activities of all of its Subcontractors to ensure that:

1. Subcontractors are complying with program requirements and achieving performance goals

2. Subcontractors are complying with fiscal requirements, such as having appropriate fiscal controls in place, and are using awards for authorized purposes.

B. Contractor can use a variety of monitoring mechanism, including limited scope audits, on-site visits, progress reports, financial reports, and review of documentation support requests for reimbursement, to meet the Contractor's monitoring objectives. The Contractor may charge federal awards for the cost of these monitoring procedures as outlined in OMB Circular A-133.

C. The Contractor shall submit to the State a copy of the procedures and any other monitoring mechanism used to monitor non-profit Subcontracts at the time of the County's annual site visit or within 60 days thereafter. Contractor shall state the frequency that non-profit Subcontracts are monitored.

D. Limited scope audits, as defined in the OMB Circular A-133, only include agreed-upon engagements that are (1) conducted in accordance with either the American Institute of Certified Public Accountants generally accepted auditing standards or attestation standards; (2) paid for and arranged by pass-through entities (counties); and (3) address one or more of the following types of compliance requirements: (i) activities allowed or unallowed; (ii) allowable costs/cost principals; (iii) eligibility; (9v) matching, level of effort and earmarking; and (v) reporting.

E. On-site visits focus on compliance and controls over compliance areas. The reviewer must make site visits to the subcontractor locations(s), and can use a variety of monitoring mechanism to document compliance requirements. The finding and the corrective action will require follow-up by the Contractor.

F. Contractor shall be responsible for any disallowance taken by the Federal Government, the State, or the California State Audit**or**, as a result of any audit exception that is related to the Contractor's responsibilities herein. Contractor shall not use funds administered by the State to repay one federal funding source with funds provided by another federal funding source, to repay federal funds with state funds, or to repay state funds with federal funds. State shall invoice Contractor 60 days after issuing the final audit report or upon resolution of an audit appeal. Contractor agrees to develop and implement any corrective action plans in a manner acceptable to the State in order to comply with recommendations contained in any audit report. Such corrective action plans shall include time-specific objectives to allow for measurement of progress and are subject to verification by the state within one year from the date of the plan.

If differences cannot be resolved between the State and Contractor regarding the terms of the financial audit settlements for funds expended under Exhibit A, Attachment I ~~A1~~, Part IV, Contractor may request an appeal in accordance with the appeal process described in Document 1J(a), "Non-DMC Audit Appeal Process," incorporated by this reference. When a financial audit is conducted by the Federal Government, the State, or the California State Auditor directly with a Subcontractor of the Contractor, and if the Subcontractor disagrees with audit disallowances related to its programs, claims or services, Contractor shall, at the Subcontractor's request, request an appeal to the State in accordance with Document 1J(a). Contractor shall include a provision in its subcontracts regarding the process by which its Subcontractors may file an appeal via the Contractors.

G. Contractors that conduct financial audits of Subcontractors, other than a Subcontractor whose funding consists entirely of non-Department funds, shall develop a process to resolve disputed financial findings and notify Subcontractors of their appeal rights pursuant to that process. This section shall not apply to those grievances or compliances arising from the financial findings of an audit or examination made by or on behalf of the State pursuant to Article IV of this Contract.

H. Pursuant to OMB Circular A-133, State may impose sanctions against the Contractor for not submitting single or program-specific audit reports, or failure to comply with all other audit requirements. The sanctions shall include:

1. Withholding a percentage of federal awards until the audit is completed satisfactorily

2. Withhold or disallowing overhead costs

3. Suspending federal awards until the audit is conducted; or

4. Terminating the federal award

Section 3. Drug Medi-Cal Financial Audits

A. In addition to the audit requirements set forth in Exhibit D(F), State may also conduct financial audits of DMC programs, exclusive of NTP services, to accomplish any of, but not limited to, the following audit objectives:

1. To review reported costs for validity, appropriate allocation methodology, and compliance with Medicaid laws and regulations;

2. To ensure that only the cost of allowable DMC activities are included in reported costs;

3. To determine the provider's usual and customary charge to the general public in accordance with CMS (The Medicare Provider Reimbursement Manual) (CMS-Pub.15), which can be obtained from the Centers for Medicare & Medicaid Services, Baltimore, Maryland, or www.cms.hhs.gov, for comparison to the DMC cost per unit;

4. To review documentation of units of service and determine the final number of approved units of service;

5. To determine the amount of clients' third-party revenue and Medi-Cal share of cost to offset allowable DMC reimbursement; and,

6. To compute final settlement based on the lower of actual allowable cost, the usual and customary charge, or the maximum allowance, in accordance with Title 22, Section 51516.1.

B. In addition to the audit requirements set forth in Exhibit D(F), State may conduct financial audits of NTP programs. For NTP services, the audits will address items A(3) through A(5) above, except that the comparison of the provider's usual and customary charge in A(3) will be to the DMC USDR rate in lieu of DMC cost per unit. In addition, these audits will include, but not be limited to:

1. For those NTP providers required to submit a cost report pursuant to W&IC Section 14124.24, a review of cost allocation methodology between NTP and other service modalities, and between DMC and other funding sources;

2. A review of actual costs incurred for comparison to services claimed;

3. A review of counseling claims to ensure that the appropriate group or individual counseling rate has been used and that counseling sessions have been billed appropriately;

4. A review of the number of clients in group sessions to ensure that sessions include no less than ~~four~~ **two** and no more than ~~ten~~ **twelve** clients at the same time, with at least one Medi-Cal client in attendance;

5. Computation of final settlement based on the lower of USDR rate or the provider's usual and customary charge to the general public; and,

6. A review of supporting service, time, financial, and patient records to verify the validity of counseling claims.

C. Contractor shall be responsible for any disallowances taken by the Federal Government, the State, or the Bureau of State Audits as a result of any audit exception that is related to its responsibilities. Contractor shall not use funds administered by the State to repay one federal funding source with funds provided by another federal funding source, or to repay federal funds with state funds, or to repay state funds with federal funds

D. Contractor agrees to promptly develop and implement any corrective action plans in a manner acceptable to the State in order to comply with recommendations contained in any audit report. Such corrective action plans shall include time-specific objectives to allow for measurement of progress and are subject to verification by the State within six months from the date of the plan.

E. Contractor, in coordination with the State, must provide follow-up on all significant findings in the audit report, including findings relating to a Subcontractor, and submit the results to the State.

If differences cannot be resolved between the State and the Contractor regarding the terms of the final financial audit settlements for funds expended under Exhibit B ~~A1~~, Contractor may request an appeal in accordance with the appeal process described in the "DMC Audit Appeal Process," Document 1J(b), incorporated by this reference. When a financial audit is conducted by the Federal Government, the State, or the Bureau of State Audits directly with a Subcontractor of the Contractor, and if the Subcontractor disagrees with audit disallowances related to its programs, claims or services, Contractor shall, at the Subcontractor's request, request an appeal to the State in accordance with Document 1J(b). Contractor shall include a provision in its subcontracts regarding the process by which a Subcontractor may file an audit appeal via the Contractor.

F. Providers of DMC services shall, upon request, make available to the State their fiscal and other records to assure that such provider have adequate recordkeeping capability and to assure that reimbursement for covered DMC services are made in accordance with Title 22, CCR, Section 51516.1. These records include, but are not limited to, matters pertaining to:

1. Provider ownership, organization, and operation;
2. Fiscal, medical, and other recordkeeping systems;
3. Federal income tax status;
4. Asset acquisition, lease, sale, or other action;
5. Franchise or management arrangements;
6. Patient service charge schedules;
7. Costs of operation;
8. Cost allocation methodology;
9. Amounts of income received by source and purpose; and,
10. Flow of funds and working capital.

G. Contractor shall retain records of utilization review activities required in Article VI herein for a minimum of three (3) years.

Exhibit B A2
Budget Detail and Payment Provisions

Part IV – Records

Section 1. General Provisions

A. Maintenance of Records

Contractor shall maintain sufficient books, records, documents, and other evidence necessary for the State to audit contract performance and contract compliance. Contractor shall make these records available to the State, upon request, to evaluate the quality and quantity of services, accessibility and appropriateness of services, and to ensure fiscal accountability. Regardless of the location or ownership of such records, they shall be sufficient to determine if costs incurred by contractor are reasonable, allowable and allocated appropriately. All records must be capable of verification by qualified auditors.

1. Contractor shall include in any contract with an audit firm a clause to permit access by the State to the working papers of the external independent auditor, and require that copies of the working papers shall be made for the State at its request.

2. Contractor shall keep adequate and sufficient financial records and statistical data to support the year-end documents filed with the State. All records must be capable of verification by qualified auditors.

3. Accounting records and supporting documents shall be retained for a three-year period from the date the year-end cost settlement report was approved by the State for interim settlement. When an audit by the Federal Government, the State, or the California State Auditor has been started before the expiration of the three-year period, the records shall be retained until completion of the audit and final resolution of all issues that arise in the audit. Final settlement shall be made at the end of the audit and appeal process. If an audit has not been completed within three years, the interim settlement shall be considered as the final settlement.

4. Financial records shall be kept so that they clearly reflect the source of funding for each type of service for which reimbursement is claimed. These documents include, but are not limited to, all ledgers, books, vouchers, time sheets, payrolls, appointment schedules, client data cards, and schedules for allocating costs. All records must be capable of verification by qualified auditors.

5. Contractor's subcontracts shall require that all Subcontractors comply with the requirements of Exhibit A, Attachment I ~~A1~~, Part V, Section 2.

6. Should a Subcontractor discontinue its contractual agreement with the Contractor, or cease to conduct business in its entirety, Contractor shall be responsible for retaining the Subcontractor's fiscal and program records for the required retention period. The State Administrative Manual (SAM) contains statutory requirements governing the retention, storage, and disposal of records pertaining to state funds. Contractor shall follow SAM requirements located at http://sam.dgs.ca.gov/TOC/1600.aspx.

   The Contractor shall retain all records required by Welfare and Institutions Code section 14124.1, 42 CFR 433.32, and California Code of Regulations, Title 22, Section 51341.1 et seq. for reimbursement of services and financial audit purposes.

7. In the expenditure of funds hereunder, and as required by 45 CFR Part 96, Contractor shall comply with the requirements of SAM and the laws and procedures applicable to the obligation and expenditure of federal and state funds.

B. Dispute Resolution Process

1. In the event of a dispute under this Exhibit A, Attachment I A1, Part IV, other than an audit dispute, Contractor shall provide written notice of the particulars of the dispute to the State before exercising any other available remedy. Written notice shall include the contract number. The Director (or designee) of the State and the County Drug or Alcohol Program Administrator (or designee) shall meet to discuss the means by which they can effect an equitable resolution to the dispute. Contractor shall receive a written response from the State within sixty (60) days of the notice of dispute. The written response shall reflect the issues discussed at the meeting and state how the dispute will be resolved.

2. In the event of a dispute over financial audit findings between the State and the Contractor, Contractor may appeal the audit in accordance with the "non- DMC Audit Appeal Process" (Document 1J(a)). When a financial audit by the Federal Government, the State, or the California State Auditor is conducted directly with a Subcontractor of the Contractor, and if the Subcontractor disagrees with audit disallowances related to its programs, claims or services, Contractor shall, at the Subcontractor's request, request an appeal to the State in accordance with Document 1J(a). Contractor shall include a provision in its subcontracts regarding the process by which a Subcontractor may file an audit appeal via the Contractor.

3. As stated in Part III, Section 3, of this Exhibit, in the event of a dispute over financial audit findings between the State and the Contractor, Contractor may appeal the audit in accordance with DMC Audit Appeal Process" (Document 1J(b)). When a financial audit by the Federal Government, the State, or the California State Auditor is conducted directly with a Subcontractor of the Contractor, and if the Subcontractor disagrees with audit disallowances related to its programs, claims or services, Contractor shall, at the Subcontractor's request, request an appeal to the State in accordance with DMC Audit Appeal Process" (Document 1J(b)). Contractor shall include a provision in its subcontracts regarding the process by which a Subcontractor may file an audit appeal via the Contractor.

4. Contractors that conduct financial audits of Subcontractors, other than a Subcontractor whose funding consists entirely of non-Department funds, shall develop a process to resolve disputed financial findings and notify Subcontractors of their appeal rights pursuant to that process. This section shall not apply to those grievances or complaints arising from the financial findings of an audit or examination made by or on behalf of the State pursuant to Part II of this Exhibit.

5. To ensure that necessary corrective actions are taken, financial audit findings are either uncontested or upheld after appeal may be used by the State during prospective contract negotiations.

Exhibit B A2
Budget Detail and Payment Provisions

Part V. Drug Medi-Cal Reimbursement Rates

A. **"Uniform Statewide Daily Reimbursement (USDR) Rate"** means the rate for NTP services based on a unit of service that is a daily treatment service provided pursuant to Title 22, Sections 51341.1 and 51516.1 and Title 9, commencing with Section 10000 (Document 3G), or the rate for individual or group counseling. The following table shows USDR rates.

Service	Type of Unit of Service (UOS)	Non-Perinatal (Regular) Rate Per UOS			Perinatal Rate Per UOS		
		FY 14/15	FY 15/16	FY 16/17	FY 14/15	FY 15/16	FY 16/17
NTP-Methadone Dosing	Daily	$10.80	$11.44	**$11.44**	$11.79	$13.58	**$13.58**
NTP-Individual Counseling (*)	One 10-minute increment	$13.48	$13.39	**$13.39**	$21.06	$21.17	**$21.17**
NTP Group Counseling (*)	One 10-minute increment	$2.91	$3.02	**$3.02**	$7.03	$5.79	**$5.79**

(*) The NTP contractors may be reimbursed for up to 200 minutes (20-10 minute increments) of individual and/or group counseling per calendar month. If medical necessity is met that requires additional NTP counseling beyond 200 minutes per calendar month, NTP contractors may bill and be reimbursed for additional counseling (in 10 minute increments). Medical justification for the additional counseling must be clearly documented in the patient record.

Reimbursement for covered NTP services shall be limited to the lower of the NTP's usual and customary charge to the general public for the same or similar services or the USDR rate.

B. **"Unit of Service"** means a face-to-face contact on a calendar day for outpatient drug free, intensive outpatient treatment, perinatal residential, and Naltrexone treatment services. Only one face-to-face service contact per day is covered by DMC except in the case of emergencies when an additional face-to-face contact may be covered for intake crisis intervention or collateral service. To count as a unit of service, the second contact shall not duplicate the services provided on the first contact, and each contact shall be clearly documented in the beneficiary's record. While the rates are approved by the State, they are subject to change through the regulation process. Units of service are identified in the following table.

Service	Type of Unit of Service (UOS)	Non-Perinatal (Regular) Rate Per UOS			Perinatal Rate Per UOS		
		FY 14/15	FY 15/16	FY 16/17	FY 14/15	FY 15/16	FY 16/17
Intensive Outpatient Treatment	Face-to-Face Visit	$56.44	$58.30	**$58.30**	$80.78	$81.22	**$81.22**
Naltrexone Treatment	Face-to-Face Visit	$19.06	$19.06	**$19.06**	NA	NA	**NA**
Outpatient Drug Free	Face-to Face Visit – Individual (per person)	$67.38	$66.93	**$66.93**	$105.32	$105.90	**$105.90**
	Face-to-Face Visit – Group (per person)	$26.23	$27.14	**$27.14**	$63.33	$52.11	**$52.11**
Perinatal Residential	Daily – Residential Day	NA	NA	**NA**	$99.43	$99.97	**$99.97**

Exhibit E A1
Additional Provisions

1. Amendment Process

A. Both the Contractor and the State may agree to amend or renegotiate the Contract.

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

C. Contract amendments will be required to change encumbered amounts for each year of a multi-year contract period, of which the first amendment will be based on the Governor's Budget Act allocation of that specific fiscal year. The signed contract from the Contractor will be due to the Department of Health Care Services within 90 days from the issuance to the County. If the signed Contract from the Contractor is not received within 90 days from the issuance to the County, DHCS may withhold all non-DMC payments under Exhibit B of this Contract until the required amendment is received by the State.

D. Contract amendments may be requested by the Contractor until May 1 of each of the contract's fiscal years. An amendment proposed by either the Contractor or the State shall be forwarded in writing to the other party.

1) The proposed amendment submitted by Contractor shall include the proposed changes, and a statement of the reason and basis for the proposed change.

2) Amendments shall be duly approved by the County Board of Supervisors or its authorized designee, and signed by a duly authorized representative.

E. Contractor acknowledges that any newly allocated funds that are in excess of the initial amount for each fiscal year may be forfeited if DHCS does not receive a fully executable contract amendment on or before June 30, 201~~5~~7.

F. State may settle costs for substance use disorder services based on the year-end cost settlement report as the final amendment to the approved single State/County contract.

2. Cancellation / Termination

A. This Agreement may be cancelled by DHCS without cause upon 30 calendar days advance written notice to the Contractor.

B. DHCS reserves the right to cancel or terminate this Agreement immediately for cause. The Contractor may submit a written request to terminate this Agreement only if DHCS substantially fails to perform its responsibilities as provided herein.

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

D. Agreement termination or cancellation shall be effective as of the date indicated in DHCS' notification to the Contractor. The notice shall stipulate any final performance, invoicing or payment requirements.

E. Upon receipt of a notice of termination or cancellation, the Contractor shall take immediate steps to stop performance and to cancel or reduce subsequent agreement costs.

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

G. In the event of changes in law that affect provisions of this Contract, the parties agree to amend the affected provisions to conform to the changes in law retroactive to the effective date of such changes in law. The parties further agree that the terms of this Contract are severable and in the event that changes in law render provisions of the Contract void, the unaffected provisions and obligations of this Contract will remain in full force and effect.

H. The following additional provisions regarding termination apply only to Exhibit A, Attachment I, Part V, of this Contract:

1) In the event the federal Department of Health and Human Services (hereinafter referred to as DHHS), or State determines Contractor does not meet the requirements for participation in the DMC Treatment Program, State will terminate payments for services provided pursuant to Exhibit A, Attachment I, Part V, of this Contract for cause.

2) All obligations to provide covered services under this Contract will automatically terminate on the effective date of any termination of this Contract. Contractor will be responsible for providing or arranging for covered services to beneficiaries until the effective date of termination or expiration of the Contract.

Contractor will remain liable for processing and paying invoices and statements for covered services and utilization review requirements prior to the expiration or termination until all obligations have been met.

3) In the event Exhibit A, Attachment I, Part V, of this Contract is nullified, Contractor shall refer DMC clients to providers who are certified to provide the type(s) of services the client has been receiving.

I. In the event this Contract is terminated, Contractor shall deliver its entire fiscal and program records pertaining to the performance of this Contract to the State, which will retain the records for the required retention period.

3. Avoidance of Conflicts of Interest by Contractor

A. DHCS intends to avoid any real or apparent conflict of interest on the part of the Contractor, subcontractors, or employees, officers and directors of the Contractor or subcontractors. Thus, DHCS reserves the right to determine, at its sole discretion, whether any information, assertion or claim received from any source indicates the existence of a real or apparent conflict of interest; and, if a conflict is found to exist, to require the Contractor to submit additional information or a plan for resolving the conflict, subject to DHCS review and prior approval.

B. Conflicts of interest include, but are not limited to:

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

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

C. If DHCS is or becomes aware of a known or suspected conflict of interest, the Contractor will be given an opportunity to submit additional information or to resolve the conflict. A Contractor with a suspected conflict of interest will have five (5) working days from the date of notification of the conflict by DHCS to provide complete information regarding the suspected conflict. If a conflict of interest is determined to exist by DHCS and cannot be resolved to the satisfaction of DHCS, the conflict will be grounds for terminating the Agreement. DHCS may, at its discretion upon receipt of a written request from the Contractor, authorize an extension of the timeline indicated herein.

D. Contractor acknowledges that state laws on conflict of interest, found in the Political Reform Act, Public Contract Code Section 10365.5, and Government Code Section 1090, apply to this Contract.

4. Freeze Exemptions

(Applicable only to local government agencies.)

A. Contractor agrees that any hiring freeze adopted during the term of this Agreement shall not be applied to the positions funded, in whole or part, by this Agreement.

B. Contractor agrees not to implement any personnel policy, which may adversely affect performance or the positions funded, in whole or part, by this Agreement.

C. Contractor agrees that any travel freeze or travel limitation policy adopted during the term of this Agreement shall not restrict travel funded, in whole or part, by this Agreement.

D. Contractor agrees that any purchasing freeze or purchase limitation policy adopted during the term of this Agreement shall not restrict or limit purchases funded, in whole or part, by this Agreement.

5. Domestic Partners

Pursuant to Public Contract Code 10295.3, no state agency may enter into any contract executed or amended after January 1, 2007, for the acquisition of goods or services in the amount of $100,000 or more with a contractor who, in the provision of benefits, discriminates between employees with spouses and employees with domestic partners, or discriminates between domestic partners and spouses of those employees.

6. Force Majeure

Neither party shall be responsible for delays or failures in performance resulting from acts beyond the control of the offending party. Such acts shall include but not be limited to acts of God, fire, flood, earthquake, other natural disaster, nuclear accident, strike, lockout, riot, freight~~,~~ ~~-~~embargo, related~~-~~utility, or governmental statutes or regulations super-imposed after the fact. If a delay or failure in performance by the Contractor arises out of a default of its Subcontractor, and if such default of its Subcontractor, arises out of causes beyond the control of both the Contractor and Subcontractor, and without the fault or negligence of either of them, the Contractor shall not be liable for damages of such delay or failure, unless the supplies or services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required performance schedule.

INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES (STATE AGENCY)

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.

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:**

TABLE 1

FEDERALLY FUNDED BENEFIT PROGRAMS	
Program	**SSA Data Exchange System(s)**
[X] Medicaid	BENDEX/SDX/EVS/SVES/SOLQ/SVES I-Citizenship /Quarters of Coverage/Prisoner Query
☐ Temporary Assistance to Needy Families (TANF)	
☐ Supplemental Nutrition Assistance Program (SNAP- formally Food Stamps)	
☐ Unemployment Compensation (Federal)	
☐ Unemployment Compensation (State)	
☐ State Child Support Agency	
☐ Low-Income Home Energy Assistance Program (LI-HEAP)	
☐ Workers Compensation	
☐ Vocational Rehabilitation Services	

☐ Foster Care (IV-E)	
☐ State Health Insurance Program (S-CHIP)	
☐ Women, Infants and Children (W.I.C.)	
[X] Medicare Savings Programs (MSP)	LIS File
[X] Medicare 1144 (Outreach)	Medicare 1144 Outreach File
☐ *Other Federally Funded, State-Administered Programs (List Below)*	
Program	SSA Data Exchange System(s)

(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 use: (a) the **tax return data** 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(1)(8); and (b) the **citizenship status data** disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3, only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants. The State Agency also acknowledges that SSA's citizenship data may be less than 50 percent current. Applicants for SSNs 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.
[X] Data will be transmitted directly between SSA and the California Office of Technology (State Transmission/Transfer Component ("STC")) by the File Transfer Management System, 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 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 "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration," attached as **Attachment 4**. 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. 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.

G. 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 call SSA's Network Customer Service Center ("NCSC") at 410-965-7777 or toll free at 1-888-772-6661 to report the actual or suspected loss. The responsible State Agency official or delegate will use the worksheet, attached as **Attachment 5**, 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 of breached and bear any costs associated with the notice or any mitigation.

H. POINTS OF CONTACT:

FOR SSA

San Francisco Regional Office:

Ellery Brown
Data Exchange Coordinator
Frank Hagel Federal Building
1221 Nevin Avenue
Richmond CA 94801
Phone: (510) 970-8243
Fax: (510) 970-8101
Email: Ellery.Brown@ssa.gov

Data Exchange Issues:

Guy Fortson
Office of Electronic Information Exchange
GD10 East High Rise
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 597-1103
Fax: (410) 597-0841
Email: guy.fortson@ssa.gov

Systems Issues:

Pamela Riley
Office of Earnings, Enumeration & Administrative Systems
DIVES/Data Exchange Branch
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-7993
Fax: (410) 966-3147
Email: Pamela.Riley@ssa.gov

Systems Security Issues:

Michael G. Johnson
Acting Director
Office of Electronic Information Exchange
Office of Strategic Services
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-0266
Fax: (410) 966-0527
Email: Michael.G.Johnson@ssa.gov

FOR STATE AGENCY

Agreement Issues:

Manuel Urbina
Chief, Security Unit
Policy Operations Branch
Medi-Cal Eligibility Division
1501 Capitol Avenue, MS 4607
Sacramento, CA 95814
Phone: (916) 650-0160
Email: Manuel.Urbina@dhcs.ca.gov

Technical Issues:

Fei Collier
Chief, Application Support Branch
Information Technology Services Division
1615 Capitol Ave, MS 6100
Sacramento, CA 95814
Phone: (916) 440-7036
Email: Fei.Collier@dhcs.ca.gov

I. DURATION: The effective date of this IEA is January 1, 2010. 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 J. below at least 30 days before the expiration and renewal of such CMPPA Agreement.

J. **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 K. 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.

K. **MODIFICATION:** Modifications to this IEA must be in writing and agreed to by the parties.

L. **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.

M. **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 – Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration
5 – PII Loss Reporting Worksheet

N. **SSA AUTHORIZED SIGNATURE:** The signatory below warrants and represents that he or she has the competent authority on behalf of SSA to enter into the obligations set forth in this IEA.

SOCIAL SECURITY ADMINISTRATION

Mary G Gallagher for

Michael G. Gallagher
Assistant Deputy Commissioner
for Budget, Finance and Management

5/13/09
Date

O. REGIONAL AND STATE AGENCY SIGNATURES:

SOCIAL SECURITY ADMINISTRATION
REGION IX

Peter D. Spencer
San Francisco Regional Commissioner

10/26/09
Date

THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

The signatory below warrants and represents that he or she has the competent authority on behalf of the State Agency to enter into the obligations set forth in this IEA.

Toby Douglas
Chief Deputy Director, Health Care Programs

10/11/09
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.

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 April 2014) 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:

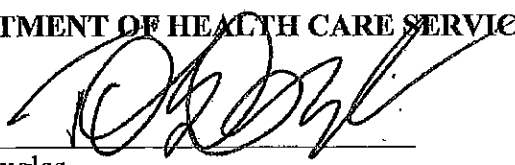
    - General System Security Design and Operating Environment
    - System Access Control
    - Automated Audit Trail
    - Monitoring and Anomaly Detection
    - Management Oversight
    - Data and Communications Security
    - Contractors of Electronic Information Exchange Partners

    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 exchanges 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



Toby Douglas
Director

10/31/14
Date

ATTACHMENT 1

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT

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 between the Social Security Administration (SSA) and the California Health and Human Services Agency (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 1137, 453, and 1106(b) of the Act (42 U.S.C. §§ 1320b-7, 653, and 1306(b)) (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)) (prisoner data);

- Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii) (Supplemental Security Income (SSI));
- 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.), 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 one or more Information Exchange Agreements (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:

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

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 number of records for each program covered under this Agreement is equal to the number of Title II, Title XVI, or Title XVIII recipients resident in the State as recorded in SSA's Annual Statistical Supplement found on the Internet at:

http://www.ssa.gov/policy/docs/statcomps/

This number will fluctuate during the term of this Agreement, corresponding to the number of Title II, Title XVI, and Title XVIII recipients added to, or deleted from, SSA databases.

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 under the Act 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 threatened 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 Performance "FY 2009 Enumeration Quality Review Report #2—The 'Numident' (January 2011)," the SSA Enumeration System database (the Master Files of SSN Holders and SSN Applications System) used for SSN matching is 98 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

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, 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 specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

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 under CHIPRA, Pub. L. 111-3, only for the purpose of determining entitlement to Medicaid and CHIP programs for new applicants.

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. 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.

9. 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 January 1, 2015 (Effective Date) through June 30, 2016 (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.

XIV. Points of Contact

A. SSA Point of Contact

Regional Office

Dolores Dunnachie, Director
San Francisco Regional Office, Center for Programs Support
1221 Nevin Avenue
Richmond CA 94801
Phone: (510) 970-8444 Fax: (510) 970-8101
Dolores.Dunnachie@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
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

Dawn S. Wiggins
Deputy Executive Director
Office of Privacy and Disclosure
Office of the General Counsel

6-12-14
Date

I certify that the SSA Data Integrity Board approved the model of this CMPPA Agreement.

Kirsten J. Moncada
Chair
SSA Data Integrity Board

7-2-14
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

11/6/14
Date

HEALTH AND HUMAN SERVICES AGENCY

Diana S. Dooley
Secretary

October 29, 2014
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 OMITTED

SENSITIVE DOCUMENT

ATTACHMENT 4

ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES

ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES FOR STATE AND LOCAL AGENCIES EXCHANGING ELECTRONIC INFORMATION WITH THE SOCIAL SECURITY ADMINISTRATION

SENSITIVE DOCUMENT

VERSION 6.0.2
April 2014

Table of Contents

RECEIVING ELECTRONIC INFORMATION FROM THE SOCIAL SECURITY ADMINISTRATION

1. Introduction

The law requires the Social Security Administration (SSA) to maintain oversight and assure the protection of information it provides to its *Electronic Information Exchange Partners* (EIEP). EIEPs are entities that have information exchange agreements with SSA.

The overall aim of this document is twofold. First, to ensure that SSA can properly certify EIEPs as compliant by the SSA security requirements, standards, and procedures expressed in this document before we grant access to SSA information in a production environment. Second, to ensure that EIEPs continue to adequately safeguard electronic information provided to them by SSA.

This document (which SSA considers SENSITIVE[1] and should only be shared with those who need it to ensure SSA-provided information is safeguarded), describes the security requirements, standards, and procedures EIEPs must meet and implement to obtain information from SSA electronically. This document helps EIEPs understand criteria that SSA uses when evaluating and certifying the system design and security features used for electronic access to SSA-provided information.

The addition, elimination, and modification of security control factors determine which level of security and due diligence SSA requires for the EIEP to mitigate risks. The emergence of new threats, attack methods, and the availability of new technology warrants frequent reviews and revisions to our System Security Requirements (SSR). Consequently, EIEPs should expect SSA's System Security Requirements to evolve in concert with the industry.

EIEPs must comply with SSA's most current SSRs to gain access to SSA-provided data. SSA will work with its partners to resolve deficiencies that occur subsequent to, and after, approval for access if updates to our security requirements cause an agency to be uncompliant. EIEPs may proactively ensure their ongoing compliance with the SSRs by periodically requesting the most current SSR package from their SSA contact. Making periodic adjustments is often necessary.

2. Electronic Information Exchange Definition

For discussion purposes herein, Electronic Information Exchange (EIE) is any electronic process in which SSA discloses information under its control to any third party for any purpose, without the specific consent of the subject individual or agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the systems of parties to electronic information sharing agreements with SSA. These processes include direct terminal access or 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.

[1] Sensitive data - "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (The Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy but is to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235)."

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 information sharing agreements executed by SSA with outside entities. Within the context of SSA's security policies and the terms of electronic information sharing agreements with SSA's EIEPs, OIS exclusively conducts and brings to closure initial security certifications and periodic security compliance reviews of EIEPs that process, maintain, transmit, or store SSA-provided information in accordance with pertinent Federal requirements which include the following (see also ***Regulatory References***):

a. The **Federal Information Security Management Act (FISMA)** requires the protection of "Federal information in contractor systems, including those systems operated by state and local governments."

b. The Social Security Administration requires EIEPs to adhere to the policies, standards, procedures, and directives published in this Systems Security Requirements (SSR) document.

   Personally Identifiable Information (PII), covered under several Federal laws and statutes, is information about an individual including, but not limited to, personal identifying information including the Social Security Number (SSN).

   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.

   However, SSA is diligent in discharging its responsibility for establishing *appropriate* administrative, technical, and physical safeguards to ensure the security, confidentiality, and availability of its records and to protect against any anticipated threats or hazards to their security or integrity.

   ***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.**

   The SSA Regional ***Data Exchange Coordinators*** (DECs) serve as a bridge between SSA and state EIEPs. In the security arena, DECs assist OIS in coordinating data exchange security review activities with state and local EIEPs; e.g., they provide points of contact with state agencies, assist 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 a suspected or actual loss of SSA-provided Personally Identifiable Information (PII).

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.

a. 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, or
- 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 SSA's associated system security requirements and procedures.

b. EIEPs must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.

c. EIEPs must use the software and/or devices provided to the EIEP only in support of the current agreement(s) between the EIEP and SSA.

d. SSA prohibits modifying any software or devices provided to the EIEPs by SSA.

e. 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.

f. 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.

g. EIEPs must store information received from SSA in a manner that, at all times, is physically and electronically secure from access by unauthorized persons.

h. The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel.

i. EIEPs must employ both physical and technological safeguards to prevent unauthorized retrieval of SSA-provided information via computer, remote terminal, or other means.

j. 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.

k. EIEPs must have an active and robust employee security awareness program, which is mandatory for all employees who access SSA-provided information.

l. EIEPs must advise employees with access to SSA-provided information of the confidential nature 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.

m. 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.

5. Systems Security Requirements

5.1 Overview

SSA must certify that the EIEP has implemented controls that meet the requirements and work as intended, before we will authorize initiating 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 Technical Systems Security Requirements (TSSRs) address management, operational, and technical aspects of security safeguards to ensure only the authorized disclosure and use of SSA-provided information by SSA's EIEPs.

SSA recommends that the EIEP develop and publish a comprehensive Systems Security Policy document that specifically addresses:

- the classification of information processed and stored within the network,
- administrative controls to protect the information stored and processed within the network,
- access to the various systems and subsystems within the network,
- Security Awareness Training,
- Employee Sanctions Policy,

- Incident Response Policy, and

- the disposal of protected information and sensitive documents derived from the system or subsystems on the network.

SSA's systems security requirements represent the current state-of-the-practice security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations, statutes, standards, and guidelines. Additionally, SSA's systems security requirements also include 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.

5.2 General System Security Design and Operating Environment

EIEPs must provide descriptions and explanations of their overall system design, configuration, security features, and operational environment and include explanations of how they conform to SSA's requirements. Explanations must include the following:

- Descriptions of the operating environment(s) in which the EIEP will utilize, maintain, and transmit SSA-provided information

- Descriptions of the business process(es) in which the EIEP will use SSA-provided information

- Descriptions of the physical safeguards employed to ensure that unauthorized personnel cannot access SSA-provided information and details of how the EIEP keeps audit information pertaining to the use and access to SSA-provided information and associated applications readily available

- Descriptions of 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 (stored or not in use)

- Descriptions of 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.)

- Descriptions of how the configurations of devices (e.g., servers, workstations, and portable devices) involving SSA-provided information comply with recognized industry standards and SSA's system security requirements

- Description of how the EIEP implements adequate security controls (e.g., passwords enforcing sufficient construction strength to defeat or minimize risk-based identified vulnerabilities)

5.3 System Access Control

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) or a security software design which is equivalent to such products. The access control software must utilize personal identification numbers (PIN) and passwords or Biometric identifiers in combination with the user's system identification code (userID). 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).

Depending on the computing platform (e.g., client/server (PC), mainframe) and the access software implementation, the terms "PIN" and "user system identification code (userID)" may be, for practical purposes, synonymous. For example, the PIN/password combination may be required for access to an individual's PC after which, the userID/password combination may be required for access to a mainframe application. A biometric identifier may supplant one element in the pair of those combinations. **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 also require more stringent password construction (e.g., passwords greater than eight characters in length requiring upper 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.

EIEPs must have management control and oversight of the function of authorizing individual user access to SSA-provided information and to oversee the process of issuing and managing access control PINs, passwords, biometric identifiers, etc. for access to the EIEP's system.

The EIEP's systems access rules must cover least privilege and individual accountability. The EIEP's rules should include procedures for access to sensitive information and transactions and functions related to it. Procedures should include control of transactions by permissions module, the assignment and limitation of system privileges, disabling accounts of separated employees (e.g., within 24 hours), individual accountability, work at home, dial-up access, and connecting to the Internet.

5.4 Automated Audit Trail

SSA requires EIEPs 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 Audit Trail System must create transaction files to capture all input from interactive internet applications which access or query SSA-provided information.

If a State Transmission Component (STC) handles and audits the EIEP's transactions with SSA, the EIEP is responsible for ensuring that the STC's audit capabilities meet SSA's requirements 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.

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 (preferably seven) years. Information in the audit file must be retrievable by an automated method. EIEPs must have the capability to make audit file information available to SSA upon request. EIEPs must back-up audit trail records on a regular basis to ensure their availability. EIEPs must apply the same level of protection to backup audit files that apply to the original files.

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 indicate to users that SSA verified the information, the EIEP's system must also capture an audit trail record of users who viewed 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.

5.5 Personally Identifiable Information (PII)

PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. 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 SSA 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 (refer to ***Incident Reporting***).

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***).

5.6 Monitoring and Anomaly Detection

SSA recommends that 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 the following:

- The EIEP's security controls continue to be effective over time
- Only authorized individuals, devices, and processes have access to SSA-provided information
- The EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions (i.e., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) as soon as they occur
- The necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes
- Upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk
- In the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions
- The 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 employees from unauthorized browsing of SSA records. SSA strongly recommends 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 then need anomaly detection to detect and monitor 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 way that it goes undetected.

If the EIEP's design does not ***currently*** 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, either 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. The system must also produce reports that allow management and/or supervisors to monitor user activity, such as the following:

- **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 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 SSNs that have no client case association within the EIEP's system **(the EIEP's management should review 100 percent of these cases).**

- **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.

- **Inquiry Activity Statistical Reports:**

  This type of report captures information about transaction usage patterns among authorized users and is a tool which 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.

5.7 Management Oversight and Quality Assurance

The EIEP must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA-provided information. They must ensure ongoing compliance with the terms of the EIEP's electronic information sharing agreement with SSA and the SSRs established for access to SSA-provided information. The entity responsible for management oversight must 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 employees and position types which require SSA-provided information to do their jobs.

The EIEP must ensure that employees granted access to SSA-provided information receive adequate training on the sensitivity of the information, associated safeguards, operating procedures, and the penalties for misuse.

SSA recommends that EIEPs establish the following job functions and require that employees tasked with these job functions do not also share the same job functions as personnel who request or use information from SSA.

- Perform periodic self-reviews to monitor the EIEP's ongoing usage of SSA-provided information.

- Perform random sampling of work activity that involves SSA-provided information to determine if the access and usage comply with SSA's requirements.

5.8 Data and Communications Security

EIEPs must 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 should align with the Standards established by the National Institute of Standards and Technology (NIST). SSA recommends the Advanced Encryption Standard (AES) or triple DES (Data Encryption Standard 3), if AES is unavailable, encryption method for securing SSA-provided information during transport. Files encrypted for external users (when using tools such as Microsoft WORD encryption,) require a key length of nine characters. We also recommend that the key (also referred to as a *password*) contain both special characters and a number. SSA requires that the EIEP deliver the key so that the key 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 Information Exchange Agreement 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. The prohibition applies to both internal and external sources who do not have a "need-to-know[2]." **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.**

EIEPs must 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

[2] Need-to-know - access to the information must be necessary for the conduct of one's official duties.

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 it unrecoverable or destroy the electronic device if they do not need to recover the data. 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:

- **Overwriting**

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 and to protect data against laboratory attacks or forensics. Please refer to ***Definitions*** for more information regarding ***Media Sanitization***). Reformatting the media does not overwrite the data.

- **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). Degaussing requires a certified tool designed for particular types of media. Certification of the tool is required 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 (refer to ***Definitions*** for more information regarding ***Media Sanitization***).

- **Physical destruction**

Physical destruction is the method 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 retention of records. The EIEP must control print media containing SSA-provided information to restrict its access to authorized employees who need such access to perform their official duties. EIEPs must destroy print media containing SSA-provided information in a secure manner when it is no longer required for business purposes. The EIEP should destroy paper documents that contain SSA-provided information by burning, pulping, shredding, macerating, or other similar means that ensure the information is unrecoverable.

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: **If SSA-provided information will be stored in a commercial**

cloud, please provide the name and address of the cloud provider. Also, please describe the security features contractually required of the cloud provider to protect SSA-provided information.

5.9 Incident Reporting

SSA requires EIEPs to develop and implement policies and procedures to respond to data breaches or PII loses. You must explain how your policies and procedures conform to SSA's requirements. The procedures must include the following information:

If the EIEP 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 and 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 the SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

The EIEP must agree to absorb all costs associated with notification and remedial actions connected to security breaches, if SSA determines that the risk presented by the breach or security incident requires the notification of the subject individuals. **SSA recommends that EIEPs seriously consider establishing incident response teams to address PII breaches.**

5.10 Security Awareness and Employee Sanctions

The EIEP must designate a department or party to take the responsibility to provide ongoing security awareness training for employees 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's responsibility for proper use and protection of SSA-provided information including its proper disposal
- 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

SSA requires the EIEP to provide security awareness training to all employees and contractors 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 or contractor who views SSA-provided data also certify that they understand the potential criminal and administrative sanctions or penalties for unlawful disclosure.

5.11 Contractors of Electronic Information Exchange Partners

As previously stated in ***The General Systems Security Standards***, contractors of the EIEP must adhere to the same security requirements as employees of the EIEP. The EIEP is responsible for the oversight of its contractors and the contractor's compliance with the security requirements. The EIEP will enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties, whereby such contractors or agents agree to abide by all relevant Federal laws, restrictions on access, use, disclosure, and the security requirements in this Agreement.

The EIEP'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 both civil and criminal sanctions pursuant to applicable Federal statutes. The EIEP 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 EIEP 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.

The EIEP must be able to provide proof of the contractual agreement If the contractor processes, handles, or transmits information provided to the EIEP by SSA or has authority to perform on the EIEP's behalf, the EIEP should clearly state the specific roles and functions of the contractor. The EIEP will provide SSA written certification that the contractor is meeting the terms of the agreement, including SSA security requirements. The certification will be subject to our final approval before redisclosing our information.

The EIEP must also require that contractors who will process, handle, or transmit information provided to the EIEP by SSA sign an agreement with the EIEP that obligates the contractor to follow the terms of the EIEP's data exchange agreement with SSA. The EIEP or the contractor must provide a copy of the data exchange agreement to each of the contractor's employees before disclosing data and make certain that the contractor's employees receive the same security awareness training as the EIEP's employees. The EIEP should maintain awareness-training records for the contractor's employees and require the same annual certification procedures.

The EIEP will be required to conduct the review of contractors and is responsible for ensuring compliance of its contractors with security and privacy requirements and limitations. As such, the EIEP will subject the contractor to ongoing security compliance

reviews that must meet SSA standards. The EIEP will conduct compliance reviews at least triennially commencing no later than three (3) years after the approved initial security certification to SSA; and must provide SSA with written documentation of recurring compliance reviews, with the contractor, subject to our approval.

If the EIEP'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:

- safeguards for sensitive information
- computer system safeguards
- security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and redisclosure of SSA-provided information
- continuous monitoring of the EIEP contractors' network infrastructures and assets

6. General -- Security Certification and Compliance Review Programs

SSA's security certification and compliance review programs are distinct processes. The certification program is a one-time process when an EIEP initially requests electronic access to SSA-provided information. The certification process entails two rigorous stages intended to ensure that technical, management, and operational security measures work as designed. SSA must ensure that the EIEPs fully conform to SSA's security requirements 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, however, ensures that the suite of security measures implemented by an EIEP to safeguard SSA-provided information remains in full compliance with SSA's security standards and requirements. 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.

6.1 The Security Certification Program

The security certification process applies to EIEPs that seek online electronic access to SSA information and consists of two general phases:

- Phase One: The Security Design Plan (SDP) phase is a formal written plan authored by the EIEP to comprehensively document its technical and non-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. OIS 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 security requirements, and providing for

more efficient security reviews.

- Phase 2: The SSA Onsite Certification phase is a formal onsite review conducted by SSA to examine the full suite of technical and non-technical security controls implemented by the EIEP to safeguard data obtained from SSA electronically (refer to ***The Certification Process***).

6.2 Documenting Security Controls in the Security Design Plan (SDP)

6.2.1 When the SDP and Risk Assessment are Required

EIEPs must submit an SDP and a security risk assessment (RA) for evaluation when one or more of the following circumstances apply. The RA must be in electronic format. It must include discussion of the measures planned or implemented to mitigate risks identified by the RA and (as applicable) risks associated with the circumstances below:

- to obtain approval for requested access to SSA-provided information for an initial agreement
- to obtain approval to reestablish previously terminated access to SSA-provided data
- to obtain approval to implement a new operating or security platform that will involve SSA-provided information
- to obtain approval for significant changes to the EIEP's organizational structure, technical processes, operational environment, data recovery capabilities, or security implementations planned or made since approval of their most recent SDP or of their most recent successfully completed security review
- 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
- to document descriptions and explanations of measures implemented as the result of a data breach or security incident
- to document descriptions and explanations of measures implemented to resolve non-compliancy issue(s)
- 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 information sharing 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 SSRs.

An SDP must satisfactorily document the EIEP's compliance with all of SSA's SSRs in order to provide the minimum level of security acceptable to SSA for its EIEP's access to SSA-provided information.

EIEP's must correct deficiencies identified through the evaluation of the SDP and submit a revised SDP that incorporates descriptions and explanations of the measures implemented to

eliminate the deficiencies. SSA cannot grant access to SSA-provided information until the EIEP corrects the deficiencies, documents the SDP, and SSA approves the revisions. The EIEP will communicate the implementation of corrective actions to SSA on a regular basis. SSA will withhold final approval until the EIEP can rectify all deficiencies.

SSA may revoke the approval of the EIEP's SDP and its access to SSA-provided information if we learn the EIEP is non-compliant with one or more SSRs. The EIEP must submit a revised SDP, which incorporates descriptions and explanations of the measures the EIEP will implement to resolve the non-compliance issue(s). The EIEP must communicate the progress of corrective action(s) to SSA on a regular basis. SSA will consider the EIEP in non-compliant status until resolution of the issue(s), the EIEP's SDP documents the corrections, and we approve the SDP. If, within a reasonable time as determined by SSA, the EIEP is unable to rectify a deficiency determined by SSA to present a substantial risk to SSA-provided information or to SSA, SSA will withhold approval of the SDP and discontinue the flow of SSA-provided information.

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 System Security Requirements (SSR) and exercise their responsibilities regarding protection of SSA-provided information.**

6.3 The Certification Process

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 non-technical and technical controls safeguard SSA-provided information from misuse and improper disclosure and that those safeguards function and work as intended.

At its discretion, SSA may request that the EIEP 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:

- a demonstration of the EIEP's implementation of each requirement
- random sampling of audit records and transactions submitted to SSA
- a walkthrough of the EIEP's data center to observe and document physical security safeguards
- a demonstration of the EIEP's implementation of electronic exchange of data with SSA
- discussions with managers/supervisors
- examination of management control procedures and reports (e.g., anomaly detection reports, etc.)
- demonstration of technical tools pertaining to user access control and if appropriate, browsing prevention, specifically:
    - If the design is based on a permission module or similar design, or it is transaction driven, the EIEP will demonstrate how the system triggers requests for information from SSA.

- If the design is based on a permission module, the EIEP will demonstrate how the process for requests for SSA-provided information prevent SSNs not present in the EIEP's system from sending requests to SSA. We will attempt to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEPs system.

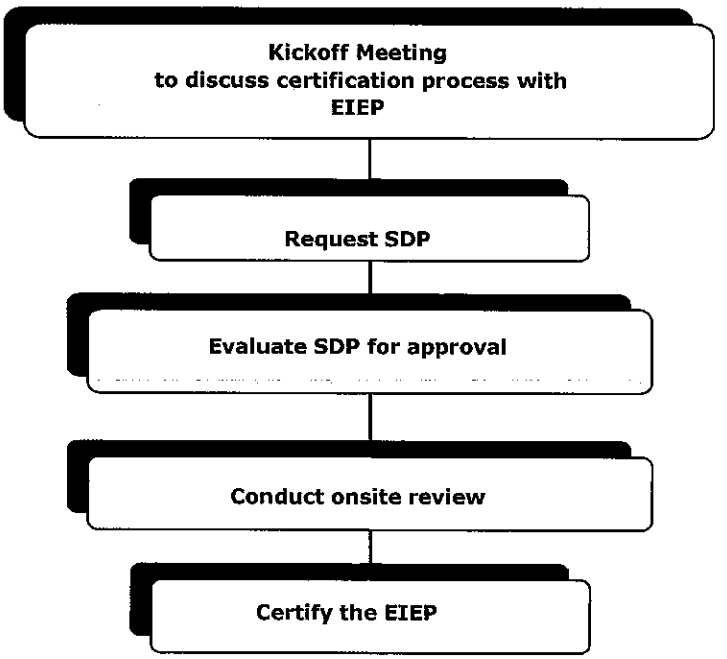
During a certification or compliance review, SSA or a certifier acting on its behalf, may request a demonstration of the EIEP's audit trail system (ATS) and its record retrieval capability. The certifier may request a demonstration of the ATS' capability to track the activity of employees who have the 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. We will 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 own in-house audit capabilities and the process used to obtain audit information from the STC.

If the EIEP employs a contractor who processes, handles, or transmits the EIEP's SSA-provided information offsite, SSA, at its discretion, may 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 exercise, 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 following is a high-level flow chart of the OIS Certification Process:

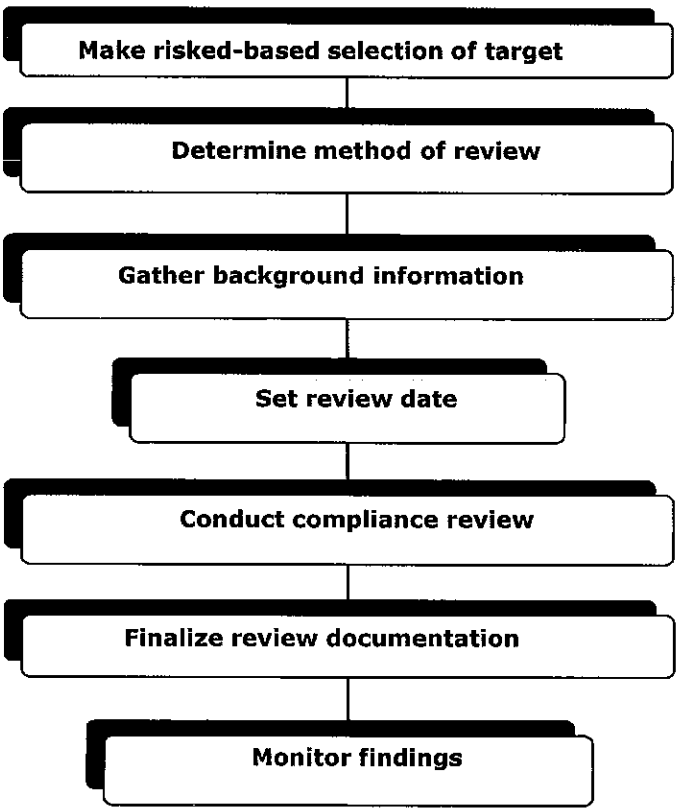


6.5 The Compliance Review Program and Process

Similar to the certification process, the compliance review program entails a rigorous process intended to ensure that EIEPs who receive electronic information from SSA are in full compliance with the Agency's security requirements and standards. As a practice, SSA attempts to conduct compliance reviews following a two to five 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 significant change in the outside EIEP's computing platform
- a violation of any of SSA's systems security requirements
- an unauthorized disclosure of SSA information by the EIEP

The following is a high-level flow chart of the OIS Compliance Review Process:



SSA may conduct onsite compliance reviews and include both the EIEP's main facility and a field office.

SSA may, also 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:

- a demonstration of the EIEP's implementation of each requirement
- random sampling of audit records and transactions submitted to SSA
- a walkthrough of the EIEP's data center to observe and document physical security safeguards
- a demonstration of the EIEP's implementation of online exchange of data with SSA
- discussions with managers/supervisors
- examination of management control procedures and reports (e.g. anomaly detection reports, etc.)
- demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention:
    - If the design uses a permission module or similar design, or is transaction driven, the EIEP will demonstrate how the system triggers requests for information from SSA.
    - If the design uses a permission module, the EIEP will demonstrate the process used to request SSA-provided information and prevent the EIEP's system from processing SSNs not present in the EIEP's system. 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, at its discretion, perform an onsite or remote review for reasons including, but not limited to the following:

- the EIEP has experienced a security breach or incident involving SSA-provided information
- the EIEP has unresolved non-compliancy issue(s)
- to review an offsite contractor's facility that processes SSA-provided information
- the EIEP is a legacy organization that has not yet been through SSAs security certification and compliance review programs
- 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 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 (i.e., the compliance review is not being conducted to address a special circumstance, such as a disclosure violation) 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 Final Report will address findings and recommendations from SSA's compliance review, which includes a plan for monitoring each issue until closure.

NOTE: SSA handles documentation provided for compliance reviews as sensitive information. 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 information sharing 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.

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. We may also use additional factors to determine whether SSA will perform an onsite or remote compliance review.

- **High/Medium Risk Criteria**

  - undocumented closing of prior review finding(s)
  - implementation of technical/operational controls that affect security of SSA-provided information (e.g. implementation of new data access method)
  - PII breach

- **Low Risk Criteria**

  - no prior review finding(s) or prior finding(s) documented as closed
  - no implementation of technical/operational controls that impact security of SSA-provided information (e.g. implementation of new data access method)
  - no PII breach

6.5.1 EIEP Compliance Review Participation

SSA may request to meet with the following persons during the compliance review:

- a sample of managers and/or supervisors 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

- the individuals responsible for performing security awareness and employee sanction functions to learn how you fulfill this requirement

- 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

- the individual(s) responsible for management oversight and quality assurance functions to confirm how your agency accomplishes this requirement
- additional individuals as deemed appropriate by SSA

6.5.2 Verification of Audit Samples

Prior to or during the compliance review, SSA will present to the EIEP a sampling of transactions previously submitted to SSA for verification. SSA requires the EIEP to verify whether each transaction was, per the terms of their agreement with SSA, legitimately submitted by a user authorized to do so.

SSA requires the EIEP to provide a written attestation of the transaction review results. The document must provide:

- confirmation that each sample transaction located in the EIEP's audit file submitted by its employee(s) was for legitimate and authorized business purposes
- an explanation for each sample transaction located in the EIEP's audit file(s) determined to have been unauthorized
- an explanation for each sample transaction not found in the EIEP's ATS

When SSA provides the sample transactions to the EIEP, detailed instructions will be included. Only an official responsible for the EIEP is to provide the attestation.

6.6 Scheduling the Onsite Review

SSA will not schedule the onsite review until we approve the EIEP's SDP. SSA will send approval notification via email. 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 follow as soon as reasonably possible.

However, the scheduling of the onsite review may depend on additional factors including:

- the reason for submission of a plan
- the severity of security issues, if any
- circumstances of the previous review, if any
- SSA workload considerations

Although the scheduling of the review is contingent upon approval of the SDP, SSA may perform an onsite review prior to approval if we determine that it is necessary to complete our evaluation of a plan.

(THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

7. Additional Definitions 0

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.

Commingling:

Commingling is the creation of a common database or repository that stores and maintains both SSA-provided and preexisting EIEP PII.

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).

Dial-up:

Sometimes used synonymously with *dial-in*, refers to digital data transmission over the wires of a local telephone network.

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:

- Disposal: Refers to the discarding (e.g., recycling) of media that contains no sensitive or confidential data.

- 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.

- 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.

  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. For example, 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.

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:

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest of the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

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 that is 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 that is 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 that 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:

The Term "Systems Process" refers to a software program module that runs in the background within an automated batch, online, or other process.

Third Party:

This term 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 information-sharing 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.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

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

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

9. Frequently Asked Questions
(Click links for answers or additional information)

1. Q: What is a breach of data?
   A: Refer also 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 SDP was submitted. Can the Onsite Review be scheduled now?
   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 is meant by 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 and RA are 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 and RA are Required.

8. Q: Is it acceptable to save SSA data 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 data 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 my agency's SVES access itself, or from the standpoint of access to all data provided to us by SSA?

A: The SDP is to encompass your agency's electronic access to SSA-provided information as per the electronic data sharing agreement between your agency and SSA. Refer to Developing the SDP.

13. Q: If we have a "transaction-driven" system, do we still need a permission module? If employees cannot initiate a query to SSA, why would we need the permission module?

A: "Transaction driven" basically means that queries automatically submit requests (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 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 the process wherein SSA performs periodic site visits to its Electronic Information Exchange Partners (EIEP) to certify whether the EIEP's 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.

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

Refer also to the Review Determination Matrix.

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 identifiable information (PII) since its previous compliance review.
- SSA rates the EIEP as a low-risk agency or state

Refer also to the Review Determination Matrix

ATTACHMENT 5

WORKSHEET FOR REPORTING LOSS OR POTENTIAL LOSS OF PERSONALLY IDENTIFIABLE INFORMATION

ATTACHMENT 5 **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):							

ATTACHMENT 5 **09/27/06**

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)**

ATTACHMENT 5 **09/27/06**

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):**