

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

**3. Cancellation/Termination**

**A. General Provisions**

- 1) As required by, if the Contractor decides not to contract with the Department, does not renew its contract, or is unable to meet the standards set by the Department, the Contractor agrees to inform the Department of this decision in writing. (Welf. & Inst. Code § 14712(c)(1).)
- 2) If the Contractor is unwilling to contract for the delivery of specialty mental health services or if the Department or Contractor determines that the Contractor is unable to adequately provide specialty mental health services or that the Contractor does not meet the standards the Department deems necessary for a mental health plan, the Department shall ensure that specialty mental health services are provided to Medi-Cal beneficiaries. (Welf. & Inst. Code § 147122(c)(2), (3).)
- 3) The Department may contract with qualifying individual counties, counties acting jointly, or other qualified entities approved by the Department for the delivery of specialty mental health services in any county that is unable or unwilling to contract with the Department. The Contractor may not subsequently contract to provide specialty mental health services unless the Department elects to contract with the Contractor. (Welf. & Inst. Code § 147122(c)(4).)
- 4) If the Contractor does not contract with the Department to provide specialty mental health services, the Department will work with the Department of Finance and the Controller to obtain funds from the Contractor in accordance with Government (Govt.) Code 30027.10. (Welf. & Inst. Code § 147122(d).)

**A. Contract Renewal**

**Exhibit E**  
**ADDITIONAL PROVISIONS**

- 1) This contract may be renewed if the Contractor continues to meet the statutory and regulatory requirements governing this contract, as well as the terms and conditions of this contract. Failure to meet these requirements shall be cause for nonrenewal of the contract. (42 C.F.R. § 438.708; Welf. & Inst. Code § 14714(b)(1).) The Department may base the decision to renew on timely completion of a mutually agreed-upon plan of correction of any deficiencies, submissions of required information in a timely manner, and/or other conditions of the contract. (Welf. & Inst. Code § 14714(b)(1).)
- 2) In the event the contract is not renewed based on the reasons specified in (1), the Department will notify the Department of Finance, the fiscal and policy committees of the Legislature, and the Controller of the amounts to be sequestered from the Mental Health Subaccount, the Mental Health Equity Account, and the Vehicle License Fee Collection Account of the Local Revenue Fund and the Mental Health Account and the Behavioral Health Subaccount of the Local Revenue Fund 2011, and the Controller will sequester those funds in the Behavioral Health Subaccount pursuant to Govt. Code § 30027.10. Upon this sequestration, the Department will use the funds in accordance with Govt. Code § 30027.10. (Welf. & Inst. Code § 14714(b)(3).)

**B. Contract Amendment Negotiations**

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

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

**D. Contract Termination**

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

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

**E. Termination of Obligations**

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

**F. Contract Disputes**

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

**4. Fulfillment of Obligation**

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

**5. Additional Provisions**

**A. Inspection Rights/Record Keeping Requirements**

**Exhibit E**  
**ADDITIONAL PROVISIONS**

- 1) Provision number seven (Audit and Record Retention) of Exhibit D(F), which is attached hereto as part of this Contract, supplements the following requirements.
- 2) The Contractor, and subcontractors, shall allow the Department, CMS, the Office of the Inspector General, the Comptroller General of the United States, and other authorized federal and state agencies, or their duly authorized designees, to evaluate Contractor's, and subcontractors', performance under this contract, including the quality, appropriateness, and timeliness of services provided, and to inspect, evaluate, and audit any and all records, documents, and the premises, equipment and facilities maintained by the Contractor and its subcontractors pertaining to such services at any time. Contractor shall allow such inspection, evaluation and audit of its records, documents and facilities, and those of its subcontractors, for 10 years from the term end date of this Contract or in the event the Contractor has been notified that an audit or investigation of this Contract has been commenced, until such time as the matter under audit or investigation has been resolved, including the exhaustion of all legal remedies, whichever is later. (See 42 C.F.R. §§ 438.3(h), 438.230(c)(3)(i-iii).) Records and documents include, but are not limited to all physical and electronic records and documents originated or prepared pursuant to Contractor's or subcontractor's performance under this Contract including working papers, reports, financial records and documents of account, beneficiary records, prescription files, subcontracts, and any other documentation pertaining to covered services and other related services for beneficiaries.
- 3) The Contractor, and subcontractors, shall retain, all records and documents originated or prepared pursuant to Contractor's or subcontractor's performance under this Contract, including beneficiary grievance and appeal records identified in Attachment 12, Section 2 and the data, information and documentation specified in 42 Code of Federal Regulations parts 438.604, 438.606, 438.608, and 438.610 for a period of no less than 10 years from the term end date of this Contract or in the event the Contractor has been notified that an audit or investigation of this Contract has been commenced, until such time as the matter under audit or investigation has been resolved, including the exhaustion

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

**B. Notices**

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

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

Lake County Behavioral Health  
Department  
P.O. Box 1024  
Lucerne, CA 95458-1024

**C. Nondiscrimination**

- 1) Consistent with the requirements of applicable federal law, such as 42 Code of Federal Regulations, part 438.3(d)(3) and (4), and state law, the Contractor shall not engage in any unlawful discriminatory practices in the admission of beneficiaries, assignments of accommodations, treatment, evaluation, employment of personnel, or in any other respect on the basis of race, color, gender, gender identity, religion, marital status, national origin, age, sexual orientation, or mental or physical handicap or disability.
- 2) The Contractor shall comply with the provisions of Section 504 of the Rehabilitation Act of 1973, as amended, pertaining to the prohibition of discrimination against qualified handicapped persons in all federally assisted programs or activities, as detailed in regulations signed by the Secretary of Health and Human Services,

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

- 3) The Contractor shall include the nondiscrimination and compliance provisions of this contract in all subcontracts to perform work under this contract.
- 4) Notwithstanding other provisions of this section, the Contractor may require a determination of medical necessity pursuant to California Code of Regulations, title 9, sections 1820.205, 1830.205 and/or 1830.210, prior to providing covered services to a beneficiary.

**D. Relationship of the Parties**

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

**E. Waiver of Default**

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

**6. Duties of the State**

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

A. Payment for Services

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

B. Reviews

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

C. Monitoring for Compliance

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

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

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



**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

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

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

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

**Exhibit E**  
**ADDITIONAL PROVISIONS**

- 2) The Department may allow the Contractor to begin delivering covered services to beneficiaries at a site subject to on-site review by the Department prior to the date of the on-site review, provided the site is operational and has any required fire clearances. The earliest date the Contractor may begin delivering covered services at a site subject to on site review by the Department is the date the Contractor requested certification of the site in accordance with procedures established by the Department, the date the site was operational, or the date a required fire clearance was obtained, whichever date is latest.
- 3) The Department may allow the Contractor to continue delivering covered services to beneficiaries at a site subject to on-site review by the Department as part of the recertification process prior to the date of the on-site review, provided the site is operational and has all required fire clearances.
- 4) Nothing in this section precludes the Department from establishing procedures for issuance of separate provider identification numbers for each of the organizational provider sites operated by the Contractor to facilitate the claiming of FFP by the Contractor and the Department's tracking of that information.

H. Excluded Providers

- 1) If the Department learns that the Contractor has a prohibited affiliation, as described in Attachment 1, Section 2, the Department:
  - a) Must notify the Secretary of the noncompliance.
  - b) May continue an existing agreement with the Contractor unless the Secretary directs otherwise.
  - c) May not renew or otherwise extend the duration of an existing agreement with the Contractor unless the Secretary provides to the State and to Congress a written statement describing compelling reasons that exist for renewing or extending the agreement despite the prohibited affiliations.
  - d) Nothing in this section must be construed to limit or otherwise affect any remedies available to the U.S. under

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

**I. Sanctions**

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

**J. Notification**

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

**K. Performance Measurement**

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

**7. State and Federal Law Governing this Contract**

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

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

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

**C. Federal law:**

- 1) Title 42 United States Code, to the extent that these requirements are applicable;
- 2) 42 C.F.R. to the extent that these requirements are applicable;
- 3) 42 C.F.R. Part 438, Medicaid Managed Care, limited to those provisions that apply to Prepaid Inpatient Health Plans (PIHPs), except for the provisions listed in paragraph D and E, below.
- 4) 42 C.F.R. § 455 to the extent that these requirements are applicable;
- 5) Title VI of the Civil Rights Act of 1964
- 6) Title IX of the Education Amendments of 1972
- 7) Age Discrimination Act of 1975
- 8) Rehabilitation Act of 1973
- 9) Americans with Disabilities Act
- 10) Section 1557 of the Patient Protection and Affordable Care Act
- 11) Deficit Reduction Act of 2005;
- 12) Balanced Budget Act of 1997.
- 13) The Contractor shall comply with the provisions of the Copeland Anti-Kickback Act, which requires that all contracts and subcontracts in excess of \$2000 for construction or repair awarded by the Contractor and its subcontractors shall include a provision for compliance with the Copeland Anti-Kickback Act.
- 14) The Contractor shall comply with the provisions of the Davis-Bacon Act, as amended, which provides that, when required by Federal Medicaid program legislation, all construction contracts awarded by

**Exhibit E**  
**ADDITIONAL PROVISIONS**

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

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

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

- 1) §438.3(b) Standard Contract Provisions – Entities eligible for comprehensive risk contracts
- 2) §438.3(c) Standard Contract Provisions - Payment
- 3) §438.3(g) Standard Contract Provisions - Provider preventable conditions
- 4) §438.3(o) Standard Contract Provisions - LTSS contract requirements
- 5) §438.3(p) Standard Contract Provisions – Special rules for HIOs
- 6) §438.3(s) Standard Contract Provisions – Requirements for MCOs, PIHPs, or PAHPs that provide covered outpatient drugs
- 7) §438.4 Actuarial Soundness
- 8) §438.5 Rate Development Standards
- 9) §438.6 Special Contract Provisions Related to Payment
- 10) §438.7 Rate Certification Submission

**Exhibit E**  
**ADDITIONAL PROVISIONS**

- 11) §438.8 Medical Loss Ratio Standards
  - 12) §438.9 Provisions that Apply to Non-emergency Medical Transportation
  - 13) §438.50 State Plan Requirements
  - 14) §438.52 Choice of MCOs, PIHPs, PAHPs, PCCMs, and PCCM entities
  - 15) §438.56 Disenrollment: requirements and limitations
  - 16) §438.70 Stakeholder engagement when LTSS is delivered through a managed care program
  - 17) 438.74 State Oversight of the Minimum MLR Requirements
  - 18) §438.104 Marketing
  - 19) §438.110 Member advisory committee
  - 20) §438.114 Emergency and Post-Stabilization
  - 21) §438.362 Exemption from External Quality Review
  - 22) §438.700-730 Basis for Imposition of Sanctions
  - 23) §438.802 Basic Requirements
  - 24) §438.810 Expenditures for Enrollment Broker Services
  - 25) §438.816 Expenditures for the beneficiary support system for enrollees using LTSS
- E. Specific provisions of 42 Code of Federal Regulations, part 438 relating to the following subjects are inapplicable to this Contract:
- 1) Long Terms Services and Supports
  - 2) Managed Long Terms Services and Supports
  - 3) Actuarially Sound Capitation Rates

**Exhibit E**  
**ADDITIONAL PROVISIONS**

- 4) Medical Loss Ratio
  - 5) Religious or Moral Objections to Delivering Services
  - 6) Family Planning Services
  - 7) Drug Formularies and Covered Outpatient Drugs
- F. Pursuant to Welfare & Institutions Code section 14704, a regulation or order concerning Medi-Cal specialty mental health services adopted by the State Department of Mental Health pursuant to Division 5 (commencing with Section 5000), as in effect preceding the effective date of this section, shall remain in effect and shall be fully enforceable, unless and until the readoption, amendment, or repeal of the regulation or order by DHCS, or until it expires by its own terms.
- G. State Law:
- 1) Division 5, Welfare & Institutions Code, to the extent that these requirements are applicable to the services and functions set forth in this contract
  - 2) Welf. & Inst. Code §§ 14680-14685.1
  - 3) Welf. & Inst. Code §§ 14700-14726
  - 4) Chapter 7, Part 3, Division 9, Welf. & Inst. Code, to the extent that these requirements are applicable to the services and functions set forth in this contract
  - 5) Cal. Code Regs., tit. 9, § 1810.100 et. seq. – Medi-Cal Specialty Mental Health Services
  - 6) Cal. Code Regs., tit. 22, §§ 50951 and 50953
  - 7) Cal. Code Regs., tit. 22, §§ 51014.1 and 51014.2

**Exhibit E – Attachment 1**  
**DEFINITIONS**

1. The following definitions and the definitions contained in California Code of Regulations, title 9, sections 1810.100-1850.535 shall apply in this contract. If there is a conflict between the following definitions and the definitions in California Code of Regulations, title 9, sections 1810.100-1850.535, the definitions below will apply.
  - A. "Advance Directives" means a written instruction, such as a living will or durable power of attorney for health care, recognized under State law (whether statutory or as recognized by the courts of the State), relating to the provision of the healthcare when the individual is incapacitated.
  - B. "Abuse" means, as the term described in, provider practices that are inconsistent with sound, fiscal, business, or medical practices, and result in an unnecessary cost to the Medi-Cal program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. It also includes beneficiary practices that result in unnecessary cost to the Medi-Cal program. (See 42 C.F.R. §§ 438.2, 455.2)
  - C. "Appeal" means a review by the Contractor of an adverse benefit determination.
  - D. "Beneficiary" means a Medi-Cal recipient who is currently receiving services from the Contractor.
  - E. "Contractor" means Lake County Behavioral Health Department.
  - F. "Covered Specialty Mental Health Services" are defined in Exhibit E, Attachment 2.
  - G. "Department" means the California Department of Health Care Services (DHCS).
  - H. "Director" means the Director of DHCS.
  - I. "Emergency" means a condition or situation in which an individual has a need for immediate medical attention, or where the potential for such need is perceived by emergency medical personnel or a public safety agency (Health & Safety Code § 1797.07).
  - J. "Fraud" means an intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to self or some other person. It includes an act that



**Exhibit E – Attachment 1  
DEFINITIONS**

constitutes fraud under applicable State and Federal law. (42 C.F.R. §§ 438.2, 455.2)

- K. "Grievance" means an expression of dissatisfaction about any matter other than adverse benefit determination. Grievances may include, but are not limited to, the quality of care or services provided, and aspects of interpersonal relationships such as rudeness of a provider or employee, or failure to respect the beneficiary's rights regardless of whether remedial action is requested. Grievance includes a beneficiary's right to dispute an extension of time proposed by the Contractor to make an authorization decision. (42 C.F.R. § 438.400)
- L. "Habilitative services and devices" help a person keep, learn, or improve skills and functioning for daily living. (45 C.F.R. § 156.115(a)(5)(i))
- M. "HHS" means the United States Department of Health and Human Service
- N. "Specialist" means a psychiatrist who has a license as a physician and surgeon in this state and shows evidence of having completed the required course of graduate psychiatric education as specified by the American Board of Psychiatry and Neurology in a program of training accredited by the Accreditation Council for Graduate Medical Education, the American Medical Association, or the American Osteopathic Association. (Cal. Code Regs., tit. 9 § 623.)
- O. A "Network Provider" means any provider, group of providers, or entity that has a network provider agreement with a Mental Health Plan, or a subcontractor, and receives Medicaid funding directly or indirectly to order, refer or render covered services as a result of the Department's contract with a Mental Health Plan. A network provider is not a subcontractor by virtue of the network provider agreement. (42 C.F.R. § 438.2)
- P. "Out-of-network provider" means a provider or group of providers that does not have a network provider agreement with a Mental Health Plan, or with a subcontractor. (A provider may be "out of network" for one Mental Health Plan, but in the network of another Mental Health Plan.)
- Q. "Out-of-plan provider" has the same meaning as out-of-network provider.
- R. "Provider" means a person or entity who is licensed, certified, or otherwise recognized or authorized under state law governing the healing arts to provide specialty mental health services and who meets the standards for

**Exhibit E – Attachment 1**  
**DEFINITIONS**

participation in the Medi-Cal program as described in California Code of Regulations, title 9, Division 1, Chapters 10 or 11 and in Division 3, Subdivision 1 of Title 22, beginning with Section 50000. Provider includes but is not limited to licensed mental health professionals, clinics, hospital outpatient departments, certified day treatment facilities, certified residential treatment facilities, skilled nursing facilities, psychiatric health facilities, general acute care hospitals, and acute psychiatric hospitals. The MHP is a provider when direct services are provided to beneficiaries by employees of the Mental Health Plan.

- S. "Overpayment" means any payment made to a network provider by a Mental Health Plan to which the provider is not entitled under Title XIX of the Act or any payment to a Mental Health Plan by a State to which the Mental Health Plan is not entitled to under Title XIX of the Act. (42 C.F.R. § 438.2)
- T. "Physician Incentive Plans" mean any compensation arrangement to pay a physician or physician group that may directly or indirectly have the effect of reducing or limiting the services provided to any plan enrollee.
- U. "PIHP" means Prepaid Inpatient Health Plan. . A Prepaid Inpatient Health Plan is an entity that:
  - 1) Provides medical services to beneficiaries under contract with the Department of Health Care Services, and on the basis of prepaid capitation payments, or other payment arrangement that does not use state plan rates;
  - 2) Provides, arranges for, or otherwise has responsibility for the provision of any inpatient hospital or institutional services for its beneficiaries; and
  - 3) Does not have a comprehensive risk contract. (42 C.F.R. § 438.2)
- V. "Rehabilitation" means a recovery or resiliency focused service activity identified to address a mental health need in the client plan. This service activity provides assistance in restoring, improving, and/or preserving a beneficiary's functional, social, communication, or daily living skills to enhance self-sufficiency or self regulation in multiple life domains relevant to the developmental age and needs of the beneficiary. Rehabilitation also includes support resources, and/or medication education. Rehabilitation may be provided to a beneficiary or a group of beneficiaries. (California's

**Exhibit E – Attachment 1**  
**DEFINITIONS**

Medicaid State Plan, State Plan Amendment 10-016, Attachment 3.1-A, Supplement 3, p. 2a.)

- W. "Satellite site" means a site owned, leased or operated by an organizational provider at which specialty mental health services are delivered to beneficiaries fewer than 20 hours per week, or, if located at a multiagency site at which specialty mental health services are delivered by no more than two employees or contractors of the provider.
- X. "Subcontract" means an agreement entered into by the Contractor with any of the following:
- 1) Any other organization or person who agrees to perform any administrative function or service for the Contractor specifically related to securing or fulfilling the Contractor's obligations to the Department under the terms of this contract.
  - 2) "Subcontractor" means an individual or entity that has a contract with an MCO, PIHP, PAHP, or PCCM entity that relates directly or indirectly to the performance of the MCO's, PIHP's, PAHP's, or PCCM entity's obligations under its contract with the State. A network provider is not a subcontractor by virtue of the network provider agreement with the MCO, PIHP, or PAHP. Notwithstanding the foregoing, for purposes of Exhibit D(F) the term "subcontractor" shall include network providers.

**Exhibit E – Attachment 2  
SERVICE DEFINITIONS**

1. The Contractor shall provide, or arrange and pay for, the following medically necessary covered Specialty Mental Health Services to beneficiaries of Lake County. Services shall be provided based on medical necessity criteria, in accordance with an individualized Client Plan, and approved and authorized according to State of California requirements. Services include:
  - A. Mental Health Services Individual or group therapies and interventions are designed to provide a reduction of mental disability and restoration, improvement or maintenance of functioning consistent with the goals of learning, development, independent living, and enhanced self-sufficiency. These services are separate from those provided as components of adult residential services, crisis intervention, crisis stabilization, day rehabilitation, or day treatment intensive. Service activities may include, but are not limited to:
    - 1) Assessment - A service activity designed to evaluate the current status of mental, emotional, or behavioral health. Assessment includes, but is not limited to, one or more of the following: mental status determination, analysis of the clinical history, analysis of relevant cultural issues and history; diagnosis; and the use of mental health testing procedures.
    - 2) Plan Development - A service activity that consists of development of client plans, approval of client plans, and/or monitoring and recording of progress.
    - 3) Therapy - A service activity that is a therapeutic intervention that focuses primarily on symptom reduction as a means to reduce functional impairments. Therapy may be delivered to an individual or group and may include family therapy at which the client is present.
    - 4) Rehabilitation - A service activity that includes, but is not limited to, assistance, improving, maintaining or restoring functional skills, daily living skills, social and leisure skills, grooming and personal hygiene skills; obtaining support resources; and/or obtaining medication education.
    - 5) Collateral - A service activity involving a significant support person in the beneficiary's life for the purpose of addressing the mental health needs of the beneficiary in terms of achieving goals of the beneficiary's client plan. Collateral may include, but is not limited

**Exhibit E – Attachment 2**  
**SERVICE DEFINITIONS**

to, consultation and training of the significant support person(s) to assist in better utilization of mental health services by the client, consultation and training of the significant support person(s) to assist in better understanding of mental illness, and family counseling with the significant support person(s) in achieving the goals of the client plan. The client may or may not be present for this service activity.

- B. Medication Support Services include prescribing, administering, dispensing and monitoring of psychiatric medications or biologicals that are necessary to alleviate the symptoms of mental illness. Service activities may include but are not limited to: evaluation of the need for medication; evaluation of clinical effectiveness and side effects; obtaining informed consent; instruction in the use, risks and benefits of, and alternatives for, medication; collateral and plan development related to the delivery of service and/or assessment for the client; prescribing, administering, dispensing and monitoring of psychiatric medications or biologicals; and medication education.
- C. Day Treatment Intensive are a structured, multi-disciplinary program of therapy that may be used as an alternative to hospitalization, or to avoid placement in a more restrictive setting, or to maintain the client in a community setting and which provides services to a distinct group of beneficiaries who receive services for a minimum of three hours per day (half-day) or more than four hours per day (full-day). Service activities may include, but are not limited to, assessment, plan development, therapy, rehabilitation and collateral. Collateral addresses the mental health needs of the beneficiary to ensure coordination with significant others and treatment providers.
- D. Day Rehabilitation services are a structured program of rehabilitation and therapy with services to improve, maintain or restore personal independence and functioning, consistent with requirements for learning and development and which provides services to a distinct group of beneficiaries who receive services for a minimum of three hours per day (half-day) or more than four hours per day (full-day). Service activities may include, but are not limited to assessment, plan development, therapy, rehabilitation and collateral. Collateral addresses the mental health needs of the beneficiary to ensure coordination with significant others and treatment providers.

**Exhibit E – Attachment 2**  
**SERVICE DEFINITIONS**

- E. Crisis Intervention services last less than 24 hours and are for, or on behalf of, a beneficiary for a condition that requires more timely response than a regularly scheduled visit. Service activities include, but are not limited to, assessment, collateral and therapy. Crisis Intervention services may either be face-to-face or by telephone with the beneficiary or the beneficiary's significant support person and may be provided anywhere in the community.
- F. Crisis Stabilization services last less than 24 hours and are for, or on behalf of, a beneficiary for a condition that requires a more timely response than a regularly scheduled visit. Service activities include but are not limited to one or more of the following: assessment, collateral, and therapy. Collateral addresses the mental health needs of the beneficiary to ensure coordination with significant others and treatment providers.
- G. Adult Residential Treatment Services are rehabilitative services provided in a non-institutional, residential setting for beneficiaries who would be at risk of hospitalization or other institutional placement if they were not receiving residential treatment services. The services include a wide range of activities and services that support beneficiaries in their effort to restore, maintain, and apply interpersonal and independent living skills and to access community support systems. Service activities may include assessment, plan development, therapy, rehabilitation, and collateral. Collateral addresses the mental health needs of the beneficiary to ensure coordination with significant others and treatment providers.
- H. Crisis Residential services provide an alternative to acute psychiatric hospital services for beneficiaries who otherwise would require hospitalization. The CRS programs for adults provide normalized living environments, integrated into residential communities. The services follow a social rehabilitation model that integrates aspects of emergency psychiatric care, psychosocial rehabilitation, milieu therapy, case management and practical social work.
- I. Psychiatric Health Facility Services—A Psychiatric Health Facility is a facility licensed under the provisions beginning with Section 77001 of Chapter 9, Division 5, Title 22 of the California Code of Regulations. "Psychiatric Health Facility Services" are therapeutic and/or rehabilitative services provided in a psychiatric health facility on an inpatient basis to beneficiaries who need acute care, which meets the criteria of Section 1820.205 of Chapter 11, Division 1, Title 9 of the California Code of Regulations, and whose physical health needs can be met in an affiliated

**Exhibit E – Attachment 2  
SERVICE DEFINITIONS**

general acute care hospital or in outpatient settings. These services are separate from those categorized as “Psychiatric Inpatient Hospital”.

- J. Intensive Care Coordination (ICC) is a targeted case management service that facilitates assessment of, care planning for and coordination of services to beneficiaries under age 21 who are eligible for the full scope of Medi-Cal services and who meet medical necessity criteria for this service. ICC service components include: assessing; service planning and implementation; monitoring and adapting; and transition. ICC services are provided through the principles of the Core Practice Model (CPM), including the establishment of the Child and Family Team (CFT) to ensure facilitation of a collaborative relationship among a youth, his/her family and involved child-serving systems. The CFT is comprised of – as appropriate, both formal supports, such as the care coordinator, providers, case managers from child-serving agencies, and natural supports, such as family members, neighbors, friends, and clergy and all ancillary individuals who work together to develop and implement the client plan and are responsible for supporting the child/youth and family in attaining their goals. ICC also provides an ICC coordinator who:
- 1) Ensures that medically necessary services are accessed, coordinated and delivered in a strength-based, individualized, family/youth driven and culturally and linguistically competent manner and that services and supports are guided by the needs of the child/youth;
  - 2) Facilitates a collaborative relationship among the child/youth, his/her family and systems involved in providing services to the child/youth;
  - 3) Supports the parent/caregiver in meeting their child/youth’s needs;
  - 4) Helps establish the CFT and provides ongoing support; and
  - 5) Organizes and matches care across providers and child serving systems to allow the child/youth to be served in his/her community
- K. Intensive Home Based Services (IHBS) are individualized, strength-based interventions designed to ameliorate mental health conditions that interfere with a child/youth’s functioning and are aimed at helping the child/youth build skills necessary for successful functioning in the home and community and improving the child/youth’s family’s ability to help the

**Exhibit E – Attachment 2**  
**SERVICE DEFINITIONS**

child/youth successfully function in the home and community. IHBS services are provided according to an individualized treatment plan developed in accordance with the Core Practice Model (CPM) by the Child and Family Team (CFT) in coordination with the family's overall service plan which may include IHBS. Service activities may include, but are not limited to assessment, plan development, therapy, rehabilitation and collateral. IHBS is provided to beneficiaries under 21 who are eligible for the full scope of Medi-Cal services and who meet medical necessity criteria for this service.

- L. Therapeutic Behavioral Services (TBS) are intensive, individualized, short-term outpatient treatment interventions for beneficiaries up to age 21. Individuals receiving these services have serious emotional disturbances (SED), are experiencing a stressful transition or life crisis and need additional short-term, specific support services to accomplish outcomes specified in the written treatment plan.
- M. Therapeutic Foster Care (TFC) Services model allows for the provision of short-term, intensive, highly coordinated, trauma informed and individualized SMHS activities (plan development, rehabilitation and collateral) to children and youth up to age 21 who have complex emotional and behavioral needs and who are placed with trained, intensely supervised and supported TFC parents. The TFC parent serves as a key participant in the therapeutic treatment process of the child or youth. The TFC parent will provide trauma informed interventions that are medically necessary for the child or youth. TFC is intended for children and youth who require intensive and frequent mental health support in a family environment. The TFC service model allows for the provision of certain SMHS activities (plan development, rehabilitation and collateral) available under the EPSDT benefit as a home-based alternative to high level care in institutional settings such as group homes and an alternative to Short Term Residential Therapeutic Programs (STRTPs).
- N. Psychiatric Inpatient Hospital Psychiatric Inpatient Hospital Services include both acute psychiatric inpatient hospital services and administrative day services. Acute psychiatric inpatient hospital services are provided to beneficiaries for whom the level of care provided in a hospital is medically necessary to diagnose or treat a covered mental illness. Administrative day services are inpatient hospital services provided to beneficiaries who were admitted to the hospital for an acute psychiatric inpatient hospital service and the beneficiary's stay at the hospital must be continued beyond the beneficiary's need for acute



**Exhibit E – Attachment 2  
SERVICE DEFINITIONS**

psychiatric inpatient hospital services due to lack of residential placement options at non-acute residential treatment facilities that meet the needs of the beneficiary.

Psychiatric inpatient hospital services are provided by SD/MC hospitals and FFS/MC hospitals. MHPs claim reimbursement for the cost of psychiatric inpatient hospital services provided by SD/MC hospitals through the SD/MC claiming system. FFS/MC hospitals claim reimbursement for the cost of psychiatric inpatient hospital services through the Fiscal Intermediary. MHPs are responsible for authorization of psychiatric inpatient hospital services reimbursed through either billing system. For SD/MC hospitals, the daily rate includes the cost of any needed professional services. The FFS/MC hospital daily rate does not include professional services, which are billed separately from the FFS/MC inpatient hospital services via the SD/MC claiming system.

- O. Targeted Case Management Targeted case management is a service that assists a beneficiary in accessing needed medical, educational, social, prevocational, vocational, rehabilitative, or other community services. The service activities may include, but are not limited to, communication, coordination and referral; monitoring service delivery to ensure beneficiary access to services and the service delivery system; monitoring of the beneficiary's progress, placement services, and plan development. TCM services may be face-to-face or by telephone with the client or significant support persons and may be provided anywhere in the community. Additionally, services may be provided by any person determined by the MHP to be qualified to provide the service, consistent with the scope of practice and state law.

**EXHIBIT F**  
**Privacy and Information Security Provisions**

**Part I: HIPAA Business Associate Addendum**

**1. Recitals**

- A. A business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), 42 U.S.C. § 17921 et seq., and their implementing privacy and security regulations at 45 C.F.R. Parts 160 and 164 ("the HIPAA regulations") between Department and Contractor arises only to the extent that Contractor performs functions or activities on behalf of the Department pursuant to this Agreement that are described in the definition of "business associate" in 45 C.F.R. § 160.103, including but not limited to utilization review, quality assurance, or benefit management.
- B. The Department wishes to disclose to Contractor certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, to be used or disclosed in the course of providing services and activities as set forth in Section 1.A. of Exhibit F, Part I of this Agreement. This information is hereafter referred to as "Department PHI".
- C. To the extent Contractor performs the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit F, Part I of this Agreement, Contractor is the Business Associate of the Department acting on the Department's behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of the Department and creates, receives, maintains, transmits, uses or discloses PHI and ePHI in the provision of such services or in the performance of such functions or activities. The Department and Contractor are each a party to this Agreement and are collectively referred to as the "parties."
- D. The purpose of this Part I is to protect the privacy and security of the PHI and ePHI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that the Department must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 C.F.R. Parts 160 and 164 and the HITECH Act.
- E. The terms used in this Part I, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

**EXHIBIT F**  
**Privacy and Information Security Provisions**

**2. Definitions**

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- D. Department PHI shall mean Protected Health Information or Electronic Protected Health Information, as defined below, accessed by Contractor in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services on behalf of the Department as specified in Section 1.A. of Exhibit F, Part I of this Agreement. The terms PHI as used in this document shall mean Department PHI.
- E. Electronic Health Records shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. § 17921 and implementing regulations.
- F. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 C.F.R. § 160.103.
- G. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 C.F.R. § 160.103.
- H. Privacy Rule shall mean the HIPAA Regulations that are found at 45 C.F.R. Parts 160 and 164, Subparts A and E.
- I. Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 C.F.R. § 160.103 and as defined under HIPAA.

**EXHIBIT F**  
**Privacy and Information Security Provisions**

- J. Required by law, as set forth under 45 C.F.R. § 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Department PHI, or confidential data utilized by Contractor to perform the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit F, Part I of this Agreement; or interference with system operations in an information system that processes, maintains or stores Department PHI.
- M. Security Rule shall mean the HIPAA regulations that are found at 45 C.F.R. Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. § 17932(h), any guidance issued by the Secretary pursuant to such Act and the HIPAA regulations.

**3. Terms of Agreement**

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

**EXHIBIT F**

**Privacy and Information Security Provisions**

- 1) **Use and disclose for management and administration.** Use and disclose Department PHI for the proper management and administration of the Contractor's business, provided that such disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware that the confidentiality of the information has been breached.
- 2) **Provision of Data Aggregation Services.** Use Department PHI to provide data aggregation services to the Department to the extent requested by the Department and agreed to by Contractor. Data aggregation means the combining of PHI created or received by the Contractor, as the Business Associate, on behalf of the Department with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the Department.

**C. Prohibited Uses and Disclosures**

- 1) Contractor shall not disclose Department PHI about an individual to a health plan for payment or health care operations purposes if the Department PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. §§ 17935(a) and 45 C.F.R. § 164.522(a).
- 2) Contractor shall not directly or indirectly receive remuneration in exchange for Department PHI, except with the prior written consent of the Department and as permitted by 42 U.S.C. § 17935(d)(2).

**D. Responsibilities of Contractor**

Contractor agrees:

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

**EXHIBIT F**  
**Privacy and Information Security Provisions**

implementation specifications and other requirements of 45 C.F.R. § 164, subpart C, in compliance with 45 C.F.R. § 164.316. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Contractor will provide the Department with its current and updated policies upon request.

- 3) **Security.** Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
  - a) Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;
  - b) Achieving and maintaining compliance with the HIPAA Security Rule (45 C.F.R. Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement; and
  - c) Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies.
- 1) **Security Officer.** Contractor shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with the Department.
- 2) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PHI by Contractor or its subcontractors in violation of the requirements of this Exhibit F, Part I.
- 3) **Reporting Unauthorized Use or Disclosure.** To report to Department any use or disclosure of Department PHI not provided for by this Exhibit F, Part I of which it becomes aware.
- 4) **Contractor's Agents and Subcontractors.**
  - a) To enter into written agreements with any agents, including subcontractors and vendors to whom Contractor provides Department PHI, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Contractor

**EXHIBIT F**

**Privacy and Information Security Provisions**

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

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

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

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

**EXHIBIT F**

**Privacy and Information Security Provisions**

- a) If Contractor maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Contractor shall provide such information in an electronic format to enable the Department to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. §17935(e). This section shall be effective as of the date that 42 U.S.C. § 17935(e) and its implementing regulations apply to the Department.
- 9) **Amendment of Department PHI.** To make any amendment(s) to Department PHI that were requested by a patient and that the Department directs or agrees should be made to assure compliance with 45 C.F.R. § 164.526, in the time and manner designated by the Department, with the Contractor being given a minimum of twenty (20) days within which to make the amendment.
- 10) **Internal Practices.** To make Contractor's internal practices, books and records relating to the use and disclosure of Department PHI available to the Department or to the Secretary, for purposes of determining the Department's compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Contractor, Contractor shall provide written notification to the Department and shall set forth the efforts it made to obtain the information.
- 11) **Documentation of Disclosures.** To document and make available to the Department or (at the direction of the Department) to an Individual such disclosures of Department PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of such PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 C.F.R. § 164.528 and 42 U.S.C. § 17935(c). If Contractor maintains electronic health records for the Department as of January 1, 2009, Contractor must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Contractor acquires electronic health records for the Department after January 1, 2009, Contractor must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting. This section shall be effective only as of the date that 42 U.S.C. § 17935(c) and its implementing regulations apply to the Department.
- 12) **Breaches and Security Incidents.** During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and



**EXHIBIT F**  
**Privacy and Information Security Provisions**

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

- a) **Initial Notice to the Department.** (1) To notify the Department **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured PHI in electronic media or in any other media if the PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. (2) To notify the Department **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement or this Exhibit F, Part I, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.
- b) Notice shall be provided to the Department Program Contract Manager and the Department Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the Department Information Security Officer. Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website ([www.dhcs.ca.gov](http://www.dhcs.ca.gov), then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link:  
  
<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx>
- c) Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI, Contractor shall take:
  - i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- d) **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI. Within 72 hours of

## **EXHIBIT F**

### **Privacy and Information Security Provisions**

the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Department Program Contract Manager and the Department Information Security Officer.

- e) **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Department Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, and the HIPAA regulations. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten(10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.
- f) **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in 42 U.S.C. § 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured Department PHI involves more than 500 residents of the State of California or its jurisdiction, Contractor shall notify the Secretary of the breach immediately upon discovery of the breach. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

**EXHIBIT F**  
**Privacy and Information Security Provisions**

- g) **Responsibility for Notification of Affected Individuals.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors and notification of the affected individuals is required under state or federal law, Contractor shall bear all costs of such notifications as well as any costs associated with the breach. In addition, the Department reserves the right to require Contractor to notify such affected individuals, which notifications shall comply with the requirements set forth in 42 U.S.C. § 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The Department Program Contract Manager and the Department Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The Department will provide its review and approval expeditiously and without unreasonable delay.
- h) **Department Contact Information.** To direct communications to the above referenced Department staff, the Contractor shall initiate contact as indicated herein. The Department reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

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

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

**EXHIBIT F**  
**Privacy and Information Security Provisions**

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

**E. Obligations of the Department**

The Department agrees to:

- 1) **Permission by Individuals for Use and Disclosure of PHI.** Provide the Contractor with any changes in, or revocation of, permission by an Individual to use or disclose Department PHI, if such changes affect the Contractor's permitted or required uses and disclosures.
- 2) **Notification of Restrictions.** Notify the Contractor of any restriction to the use or disclosure of Department PHI that the Department has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the Contractor's use or disclosure of PHI.
- 3) **Requests Conflicting with HIPAA Rules.** Not request the Contractor to use or disclose Department PHI in any manner that would not be permissible under the HIPAA regulations if done by the Department.
- 4) **Notice of Privacy Practices.** Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 C.F.R. § 164.520, as well as any changes to such notice. Visit the DHCS Privacy Office to view the most current Notice of Privacy Practices at: <http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx> or the DHCS website at [www.dhcs.ca.gov](http://www.dhcs.ca.gov) (select "Privacy in the right column and "Notice of Privacy Practices" on the right side of the page).

**F. Audits, Inspection and Enforcement**

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

**EXHIBIT F**  
**Privacy and Information Security Provisions**

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

**G. Termination**

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

**EXHIBIT F**  
**Privacy and Information Security Provisions**

**Part II: Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA**

**1. Recitals**

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

**EXHIBIT F****Privacy and Information Security Provisions**

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

**2. Definitions**

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

## **EXHIBIT F**

### **Privacy and Information Security Provisions**

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

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

### **3. Terms of Agreement**

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

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

#### **B. Responsibilities of Contractor**

Contractor agrees:

- 1) **Nondisclosure.** Not to use or disclose Department PI or PII other than as permitted or required by this Agreement or as required by applicable state and federal law.
- 2) **Safeguards.** To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of Section 3, Security, below. Contractor will provide DHCS with its current policies upon request.
- 3) **Security.** Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
  - a) Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements; and



## EXHIBIT F

### Privacy and Information Security Provisions

- b) Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies.
  - c) If the data obtained by User(s) from DHCS includes PII, User(s) shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement (IEA), which are attached as Attachment B and are incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide DHCS PII agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information.
- 4) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PI or PII by Contractor or its subcontractors in violation of this Exhibit F, Part II.
  - 5) **Contractor's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit F, Part II on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of Department PI or PII to the subcontractor.
  - 6) **Availability of Information to DHCS.** To make Department PI and PII available to the Department for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of Department PI and PII. If Contractor receives Department PII, upon request by DHCS, Contractor shall provide DHCS with a list of all employees, contractors and agents who have access to Department PII, including employees, contractors and agents of its subcontractors and agents.
  - 7) **Cooperation with DHCS.** With respect to Department PI, to cooperate with and assist the Department to the extent necessary to ensure the Department's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of Department PI, correction of

## EXHIBIT F

### Privacy and Information Security Provisions

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

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

**EXHIBIT F**

**Privacy and Information Security Provisions**

- ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- d) **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI . Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Department Program Contract Manager and the Department Information Security Officer:
- e) **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Department Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten(10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.
- f) **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PI or PII is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in CIPA, § 1798.29(a) – (d) and as may be required under the IEA. Contractor shall bear all costs of required notifications to individuals as well as any costs associated with the breach. The Department Program Contract Manager and the Department Information Security Officer and Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications

**EXHIBIT F**  
**Privacy and Information Security Provisions**

are made. The Department will provide its review and approval expeditiously and without unreasonable delay. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

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

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

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

**EXHIBIT F**  
**Privacy and Information Security Provisions**

**Part III: Miscellaneous Terms and Conditions Applicable to Exhibit F**

**1. Disclaimer**

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

**2. Amendment**

A. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit F may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit F embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations. The Department may terminate this Agreement upon thirty (30) days written notice in the event:

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

**3. Judicial or Administrative Proceedings**

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

**4. Assistance in Litigation or Administrative Proceedings**

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

**EXHIBIT F**  
**Privacy and Information Security Provisions**

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

**5. No Third-Party Beneficiaries**

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

**6. Interpretation**

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

**7. Conflict**

In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Contractor must comply within a reasonable period of time with changes to these standards that occur after the effective date of this Agreement.

**8. Regulatory References**

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

**9. Survival**

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

**10. No Waiver of Obligations**

No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

**11. Audits, Inspection and Enforcement**

**EXHIBIT F**  
**Privacy and Information Security Provisions**

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

**12. Due Diligence**

Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit F and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit F.

**13. Term**

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

**14. Effect of Termination**

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

**EXHIBIT F**  
**Privacy and Information Security Provisions**

**Attachment A**  
**Business Associate Data Security Requirements**

**1. Personnel Controls**

- A. **Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of the Department, or access or disclose Department PHI or PI must complete information privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following termination of this Agreement.
- B. **Employee Discipline.** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. **Confidentiality Statement.** All persons that will be working with Department PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to Department PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for Department inspection for a period of six (6) years following termination of this Agreement.
- D. **Background Check.** Before a member of the workforce may access Department PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years.

**2. Technical Security Controls**

- A. **Workstation/Laptop encryption.** All workstations and laptops that store Department PHI or PI either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the Department Information Security Office.
- B. **Server Security.** Servers containing unencrypted Department PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.



**EXHIBIT F****Privacy and Information Security Provisions**

- C. **Minimum Necessary.** Only the minimum necessary amount of Department PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. **Removable media devices.** All electronic files that contain Department PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.
- E. **Antivirus software.** All workstations, laptops and other systems that process and/or store Department PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- F. **Patch Management.** All workstations, laptops and other systems that process and/or store Department PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.
- G. **User IDs and Password Controls.** All users must be issued a unique user name for accessing Department PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
- 1) Upper case letters (A-Z)
  - 2) Lower case letters (a-z)
  - 3) Arabic numerals (0-9)
  - 4) Non-alphanumeric characters (punctuation symbols)
- H. **Data Destruction.** When no longer needed, all Department PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the Department Information Security Office.

**EXHIBIT F**  
**Privacy and Information Security Provisions**

- I. **System Timeout.** The system providing access to Department PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
  - J. **Warning Banners.** All systems providing access to Department PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
  - K. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for Department PHI or PI, or which alters Department PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Department PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
  - L. **Access Controls.** The system providing access to Department PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.
  - M. **Transmission encryption.** All data transmissions of Department PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing Department PHI can be encrypted. This requirement pertains to any type of Department PHI or PI in motion such as website access, file transfer, and E-Mail.
  - N. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting Department PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.
3. **Audit Controls**
- A. **System Security Review.** Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Department PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.
  - B. **Log Reviews.** All systems processing and/or storing Department PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
  - C. **Change Control.** All systems processing and/or storing Department PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

**EXHIBIT F**  
**Privacy and Information Security Provisions**

**4. Business Continuity / Disaster Recovery Controls**

- A. **Emergency Mode Operation Plan.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of Department PHI or PI held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.
- B. **Data Backup Plan.** Contractor must have established documented procedures to backup Department PHI to maintain retrievable exact copies of Department PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore Department PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of Department data.

**5. Paper Document Controls**

- A. **Supervision of Data.** Department PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Department PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. **Escorting Visitors.** Visitors to areas where Department PHI or PI is contained shall be escorted and Department PHI or PI shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** Department PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. **Removal of Data.** Only the minimum necessary Department PHI or PI may be removed from the premises of the Contractor except with express written permission of the Department. Department PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Contractor's locations to another of Contractor's locations.
- E. **Faxing.** Faxes containing Department PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.
- F. **Mailing.** Mailings containing Department PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible.

**EXHIBIT F**

**Privacy and Information Security Provisions**

Mailings which include 500 or more individually identifiable records of Department PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of the Department to use another method is obtained.



---

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

---

- A. PURPOSE:** The purpose of this Information Exchange Agreement ("IEA") is to establish terms, conditions, and safeguards under which SSA will disclose to the State Agency certain information, records, or data (herein "data") to assist the State Agency in administering certain federally funded, state-administered benefit programs (including state-funded, state supplementary payment programs under Title XVI of the Social Security Act) identified in this IEA. By entering into this IEA, the State Agency agrees to comply with:
- the terms and conditions set forth in the Computer Matching and Privacy Protection Act Agreement ("CMPPA Agreement") attached as **Attachment 1**, governing the State Agency's use of the data disclosed from SSA's Privacy Act System of Records; and
  - all other terms and conditions set forth in this IEA and Attachments 2 through 6.
- B. PROGRAMS AND DATA EXCHANGE SYSTEMS:** (1) The State Agency will use the data received or accessed from SSA under this IEA for the purpose of administering the federally funded, state-administered programs identified in **Table 1** below. In **Table 1**, the State Agency has identified: (a) each federally funded, state-administered program that it administers; and (b) each SSA data exchange system to which the State Agency needs access in order to administer the identified program. The list of SSA's data exchange systems is attached as **Attachment 2**. **Attachment 2** provides a brief explanation of each system, as well as use parameters, as necessary.

**TABLE 1**

<b>FEDERALLY FUNDED BENEFIT PROGRAMS</b>	
<b>Program</b>	<b>SSA Data Exchange System(s)</b>
<input checked="" type="checkbox"/> Medicaid	BENDEX/SDX/SVES IV/SOLQ/SVES-1-Citizenship/Quarters of Coverage/PUPS
<input type="checkbox"/> Temporary Assistance to Needy Families (TANF)	
<input type="checkbox"/> Supplemental Nutrition Assistance Program (SNAP- formerly Food Stamps)	
<input type="checkbox"/> Unemployment Compensation	
<input type="checkbox"/> State Child Support Agency	
<input type="checkbox"/> Low-Income Home Energy Assistance Program (LI-HEAP)	
<input type="checkbox"/> Workers Compensation	
<input type="checkbox"/> Vocational Rehabilitation Services	



Exhibit F, Attachment B

<input type="checkbox"/> Foster Care (IV-E)	
<input checked="" type="checkbox"/> State Children's Health Insurance Program (CHIP)	BENDEX/SDX/SVES IV, SVES-1 Citizenship
<input type="checkbox"/> Women, Infants and Children (W.I.C.)	
<input checked="" type="checkbox"/> Medicare Savings Programs (MSP)	LIS File
<input checked="" type="checkbox"/> Medicare 1144 (Outreach)	Medicare 1144 Outreach File
<input checked="" type="checkbox"/> Other Federally Funded, State-Administered Programs (List Below)	
Program	SSA Data Exchange System(s)
Medi-Cal Access Program (MCAP)	BENDEX/SDX/SVES IV

(2) The State Agency will use each identified data exchange system only for the purpose of administering the specific program for which access to the data exchange system is provided. SSA data exchange systems are protected by the Privacy Act and Federal law prohibits the use of SSA's data for any purpose other than the purpose of administering the specific program for which such data is disclosed. In particular, the State Agency will:

- a) use the tax return data disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a program listed in 26 U.S.C. § 6103(1)(7) and (8).
- b) use citizenship status data disclosed by SSA only to determine entitlement of new applicants to: (a) the Medicaid program and CHIP pursuant to the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA to receive the SSA Data Set through the Centers for Medicare & Medicaid Services' (CMS) Federal Data Services Hub (Hub).

Applicants for Social Security numbers (SSN) report their citizenship data at the time they apply for their SSNs; there is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files a claim for benefits.

- C. **PROGRAM QUESTIONNAIRE:** Prior to signing this IEA, the State Agency will complete and submit to SSA a program questionnaire for each of the federally funded, state-administered programs checked in Table 1 above. SSA will not disclose any data under this IEA until it has received and approved the completed program questionnaire for each of the programs identified in Table 1 above.



**D. TRANSFER OF DATA:** SSA will transmit the data to the State Agency under this IEA using the data transmission method identified in Table 2 below:

**TABLE 2**

TRANSFER OF DATA
<input type="checkbox"/> Data will be transmitted directly between SSA and the State Agency.
<input checked="" type="checkbox"/> Data will be transmitted directly between SSA and The California Office of Technology (State Transmission/Transfer Component ("STC")) by File Transfer Management System (FTMS), a secure mechanism approved by SSA. The STC will serve as the conduit between SSA and the State Agency pursuant to the State STC Agreement.
<input type="checkbox"/> Data will be transmitted directly between SSA and CMS' Hub by a secure method of transfer approved by SSA. CMS will transmit the SSA Data Set between SSA and the State Agency pursuant to an agreement between SSA and CMS regarding the use of the Hub.
<input type="checkbox"/> Data will be transmitted <u>[select one: directly between SSA and the Interstate Connection Network ("ICON") or through the [name of STC Agency/Vendor] as the conduit between SSA and the Interstate Connection Network ("ICON")]</u> . ICON is a wide area telecommunications network connecting state agencies that administer the state unemployment insurance laws. When receiving data through ICON, the State Agency will comply with the "Systems Security Requirements for SSA Web Access to SSA Information Through the ICON," attached as Attachment 3.

**E. SECURITY PROCEDURES:** The State Agency will comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), and related National Institute of Standards and Technology guidelines. In addition, the State Agency will comply with SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," attached as Attachment 4, as well as the Security Certification Requirements for use of the SSA Data Set transmitted via CMS' Hub, attached as Attachment 5. The SSA security controls identified under Attachment 4 of this IEA prevail for all SSA data received by the State Agency, as identified in Table 1 of this IEA. For any tax return data, the State Agency will also comply with the "Tax Information Security Guidelines for Federal, State and Local Agencies," Publication 1075, published by the Secretary of the Treasury and available at the following Internal Revenue Service (IRS) website: <http://www.irs.gov/pub/irs-pdf/p1075.pdf>. This IRS Publication 1075 is incorporated by reference into this IEA.

**F. STATE AGENCY'S RESPONSIBILITIES:** The State Agency will not direct individuals to SSA field offices to obtain data that the State Agency is authorized to receive under this IEA in accordance with Table 1. Where disparities exist between individual-supplied data and SSA's data, the State Agency will take the following steps before referring the individual to an SSA field office:





## Exhibit F, Attachment B

- Check its records to be sure that the data of the original submission has not changed (e.g., last name recently changed);
- Contact the individual to verify the data submitted is accurate; and,
- Consult with the SSA Regional Office Contact to discuss options before advising individuals to contact SSA for resolution. The Regional Office Contact will inform the State Agency of the current protocol through which the individual should contact SSA, i.e., visiting the field office, calling the national network service number, or creating an online account via my Social Security.

**G. CONTRACTOR/AGENT RESPONSIBILITIES:** The State Agency will restrict access to the data obtained from SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this IEA. At SSA's request, the State Agency will obtain from each of its contractors and agents a current list of the employees of its contractors and agents who have access to SSA data disclosed under this IEA. The State Agency will require its contractors, agents, and all employees of such contractors or agents with authorized access to the SSA data disclosed under this IEA, to comply with the terms and conditions set forth in this IEA, and not to duplicate, disseminate, or disclose such data without obtaining SSA's prior written approval. In addition, the State Agency will comply with the limitations on use, duplication, and redisclosure of SSA data set forth in Section IX. of the CMPPA Agreement, especially with respect to its contractors and agents.

## **H. SAFEGUARDING AND REPORTING RESPONSIBILITIES FOR PERSONALLY IDENTIFIABLE INFORMATION ("PII"):**

1. The State Agency will ensure that its employees, contractors, and agents:
  - a. properly safeguard PII furnished by SSA under this IEA from loss, theft, or inadvertent disclosure;
  - b. understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee, contractor, or agent is at his or her regular duty station;
  - c. ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected;
  - d. send emails containing PII only if encrypted or if to and from addresses that are secure; and
  - e. limit disclosure of the information and details relating to a PII loss only to those with a need to know.
2. If an employee of the State Agency or an employee of the State Agency's contractor or agent becomes aware of suspected or actual loss of PII, he or she must immediately contact the State Agency official responsible for Systems Security designated below or his or her delegate. That State Agency official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact identified below. If, for any reason, the responsible State Agency official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center at 1-877-697-4889. The responsible State Agency official or delegate will use the worksheet, attached as Attachment 6, to quickly gather and



## Exhibit F, Attachment B

organize information about the incident. The responsible State Agency official or delegate must provide to SSA timely updates as any additional information about the loss of PII becomes available.

3. SSA will make the necessary contact within SSA to file a formal report in accordance with SSA procedures. SSA will notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of PII related to a data exchange under this IEA occurs.
4. If the State Agency experiences a loss or breach of data, it will determine whether or not to provide notice to individuals whose data has been lost or breached and bear any costs associated with the notice or any mitigation.

### I. POINTS OF CONTACT:

#### FOR SSA

**San Francisco Regional Office:**  
Nancy Borjon  
Data Exchange Coordinator  
Frank Hagel Federal Building  
1221 Nevin Avenue  
Richmond, CA 94801  
Phone: (510) 970-8256  
Fax: (510) 970-8101  
Email: [Nancy.Borjon@ssa.gov](mailto:Nancy.Borjon@ssa.gov)

**Program and Policy Issues:**  
Michael Wilkins  
State Liaison Program Manager  
Office of Retirement and Disability Policy  
Office of Data Exchange and Policy  
Publications  
Office of Data Exchange  
3609 Annex Building  
6401 Security Boulevard  
Baltimore, MD 21235  
Phone: (410) 966-4965  
Fax: (410) 966-4054  
Email: [Michael.Wilkins@ssa.gov](mailto:Michael.Wilkins@ssa.gov)

**Systems Issues:**  
Michelle J. Anderson, Branch Chief  
DBIAE/Data Exchange and Verification  
Branch

**Data Exchange Issues:**  
Sarah Reagan  
Government Information Specialist  
Office of the General Counsel  
Office of Privacy and Disclosure  
617 Altmeyer  
6401 Security Boulevard  
Baltimore, MD 21235  
Phone: (410) 965-9127  
Fax: (410) 594-0115  
Email: [Sarah.Reagan@ssa.gov](mailto:Sarah.Reagan@ssa.gov)

**Systems Security Issues:**  
Sean Hagan, Acting Director  
Division of Compliance and  
Assessments  
Office of Information Security  
Office of Systems  
Social Security Administration  
3829 Annex Building  
6401 Security Boulevard  
Baltimore, MD 21235  
Phone: (410) 965-4519  
Fax: (410) 597-0845  
Email: [Sean.Hagan@ssa.gov](mailto:Sean.Hagan@ssa.gov)



Exhibit F, Attachment B

Office of Information Technology Business  
Support  
Office of Systems  
3-D-I Robert M. Ball Building  
6401 Security Boulevard  
Baltimore, MD 21235  
Phone: (410) 965-5943  
Fax: (410) 966-3147  
Email: [Michelle.L.Anderson@ssa.gov](mailto:Michelle.L.Anderson@ssa.gov)

**FOR STATE AGENCY**

**Agreement Issues:**

Rocky Evans  
Chief, Eligibility Administration Section  
Program Review Branch  
Medi-Cal Eligibility Division (MCEID)  
1501 Capitol Avenue  
Sacramento, CA 95814  
Phone: (916) 319-8434  
Fax: (916) 552-9477  
Email: [Rocky.Evans@dhcs.ca.gov](mailto:Rocky.Evans@dhcs.ca.gov)

**Technical Issues:**

YK Chalameherla  
Chief, Application Development &  
Support Branch  
Enterprise Innovative Technology  
Services (EITS)  
1501 Capitol Avenue  
Sacramento, CA 95814  
Phone: (916) 322-8044  
Fax: (916) 440-7065  
Email: [YK.Chalameherla@dhcs.ca.gov](mailto:YK.Chalameherla@dhcs.ca.gov)

Sean Wieland  
Chief, Business & Application  
Integration Section  
Enterprise Innovative Technology  
Services (EITS)  
1501 Capitol Avenue  
Sacramento, CA 95814  
Phone: (916) 550-7088  
Fax: (916) 440-7065  
Email: [Sean.Wieland@dhcs.ca.gov](mailto:Sean.Wieland@dhcs.ca.gov)

- J. DURATION:** The effective date of this IEA is March 6, 2017. This IEA will remain in effect for as long as: (1) a CMPPA Agreement governing this IEA is in effect between SSA and the State or the State Agency; and (2) the State Agency submits a certification in accordance with Section K. below at least 30 days before the expiration and renewal of such CMPPA Agreement.
- K. CERTIFICATION AND PROGRAM CHANGES:** At least 30 days before the expiration and renewal of the State CMPPA Agreement governing this IEA, the State Agency will certify in writing to SSA that: (1) it is in compliance with the terms and conditions of this IEA; (2) the data exchange processes under this IEA have been and will be conducted without change; and (3) it will, upon SSA's request, provide audit reports or other documents that demonstrate review and oversight activities. If there are substantive changes in any of the programs or data exchange processes listed in this IEA, the parties will modify the IEA in



## Exhibit F, Attachment B

accordance with Section L. below and the State Agency will submit for SSA's approval new program questionnaires under Section C. above describing such changes prior to using SSA's data to administer such new or changed program.

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

**M. TERMINATION:** The parties may terminate this IEA at any time upon mutual written consent. In addition, either party may unilaterally terminate this IEA upon 90 days advance written notice to the other party. Such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow under this IEA, or terminate this IEA, if SSA, in its sole discretion, determines that the State Agency (including its employees, contractors, and agents) has: (1) made an unauthorized use or disclosure of SSA-supplied data; or (2) violated or failed to follow the terms and conditions of this IEA or the CMPPA Agreement.

**N. INTEGRATION:** This IEA, including all attachments, constitutes the entire agreement of the parties with respect to its subject matter. There have been no representations, warranties, or promises made outside of this IEA. This IEA shall take precedence over any other document that may be in conflict with it.

### ATTACHMENTS

- 1 - CMPPA Agreement
- 2 - SSA Data Exchange Systems
- 3 - Systems Security Requirements for SSA Web Access to SSA Information Through ICON
- 4 - Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration
- 5 - Security Certification Requirements for use of the SSA Data Set Transmitted via CMS' Hub
- 6 - PII Loss Reporting Worksheet



Exhibit F, Attachment B

- O. **AUTHORIZED SIGNATURES:** The signatories below warrant and represent that they have competent authority on behalf of their respective agency to enter into the obligations set forth in this IEA.

SOCIAL SECURITY ADMINISTRATION  
REGION IX



Grace M. Kim  
Regional Commissioner

05/03/2017

Date

THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES



Jennifer Kent  
Director, California Department of Health Care Services

4/7/17

Date



**CERTIFICATION OF COMPLIANCE  
FOR  
THE INFORMATION EXCHANGE AGREEMENT  
BETWEEN  
THE SOCIAL SECURITY ADMINISTRATION (SSA)  
AND  
THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES (STATE  
AGENCY)  
(State Agency Level)**

In accordance with the terms of the Information Exchange Agreement (IEA/F) between SSA and the State Agency, the State Agency, through its authorized representative, hereby certifies that, as of the date of this certification:

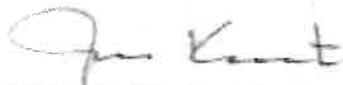
1. The State Agency is in compliance with the terms and conditions of the IEA/F;
2. The State Agency has conducted the data exchange processes under the IEA/F without change, except as modified in accordance with the IEA/F;
3. The State Agency will continue to conduct the data exchange processes under the IEA/F without change, except as may be modified in accordance with the IEA/F;
4. Upon SSA's request, the State Agency will provide audit reports or other documents that demonstrate compliance with the review and oversight activities required under the IEA/F and the governing Computer Matching and Privacy Protection Act Agreement;  
and
5. In compliance with the requirements of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," (last updated July 2015) Attachment 4 to the IEA/F, as periodically updated by SSA, the State Agency has not made any changes in the following areas that could potentially affect the security of SSA data:
  - General System Security Design and Operating Environment
  - System Access Control
  - Automated Audit Trail
  - Monitoring and Anomaly Detection
  - Management Oversight
  - Data and Communications Security
  - Contractors of Electronic Information Exchange Partners
  - Cloud Service Providers for Electronic Information Exchange Partners

The State Agency will submit an updated Security Design Plan at least 30 days prior to making any changes to the areas listed above and provide updated contractor employee lists before allowing new employees' access to SSA provided data.

6. The State Agency agrees that use of computer technology to transfer the data is more economical, efficient, and faster than using a manual process. As such, the State Agency will continue to utilize data exchange to obtain data it needs to administer the programs for which it is authorized, under the IEA/F. Further, before directing an individual to an SSA field office to obtain data, the State Agency will verify that the information is submitted to SSA via data exchange is correct, and verify with the individual that the information he/she supplied is accurate. The use of electronic data exchange expedites program administration and limits SSA field office traffic.

The signatory below warrants and represents that he or she is a representative of the State Agency duly authorized to make this certification on behalf of the State Agency.

**DEPARTMENT OF HEALTH CARE SERVICES OF CALIFORNIA**

  
\_\_\_\_\_  
Jennifer Kent  
Director

5/17/17  
\_\_\_\_\_  
Date

**ATTACHMENT 1**

**COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT  
(CMPPA)**



Exhibit F, Attachment B

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT  
BETWEEN  
THE SOCIAL SECURITY ADMINISTRATION  
AND  
THE HEALTH AND HUMAN SERVICES AGENCY  
OF CALIFORNIA

I. Purpose and Legal Authority

A. Purpose

This Computer Matching and Privacy Protection Act (CMPPA) Agreement (Agreement) between the Social Security Administration (SSA) and the Health and Human Services Agency of California (State Agency) sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein as "data") made by SSA to the State Agency that administers federally funded benefit programs, including those under various provisions of the Social Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), as well as the state-funded state supplementary payment programs under Title XVI of the Act. The terms and conditions of this Agreement ensure that SSA makes such disclosures of data, and the State Agency uses such disclosed data, in accordance with the requirements of the Privacy Act of 1974, as amended by the CMPPA of 1988, 5 U.S.C. § 552a.

Under section 1137 of the Act, the State Agency is required to use an income and eligibility verification system to administer specified federally funded benefit programs, including the state-funded state supplementary payment programs under Title XVI of the Act. To assist the State Agency in determining entitlement to and eligibility for benefits under those programs, as well as other federally funded benefit programs, SSA discloses certain data about applicants (and in limited circumstances, members of an applicant's household), for state benefits from SSA Privacy Act Systems of Records (SOR) and verifies the Social Security numbers (SSN) of the applicants.

B. Legal Authority

SSA's authority to disclose data and the State Agency's authority to collect, maintain, and use data protected under SSA SORs for specified purposes is:

- Sections 453, 1106(b), and 1137 of the Act (42 U.S.C. §§ 653, 1306(b), and 1320b-7) (income and eligibility verification data);
- 26 U.S.C. § 6103(l)(7) and (8) (tax return data);
- Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 402(x)(3)(B)(iv)) and Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii)) (prisoner data);

- Section 205(r)(3) of the Act (42 U.S.C. § 405(r)(3)) and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2) (death data);
- Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645) (quarters of coverage data);
- Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA), Pub. L. 111-3 (citizenship data); and
- Routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3) (data necessary to administer other programs compatible with SSA programs).

This Agreement further carries out section 1106(a) of the Act (42 U.S.C. § 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the CMPPA, related Office of Management and Budget (OMB) guidelines, the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3541, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283), and related National Institute of Standards and Technology (NIST) guidelines, which provide the requirements that the State Agency must follow with regard to use, treatment, and safeguarding of data.

## II. Scope

- A. The State Agency will comply with the terms and conditions of this Agreement and the Privacy Act, as amended by the CMPPA.
- B. The State Agency will execute an Information Exchange Agreement (IEA) with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by the State Agency, the data elements that will be disclosed, and the data protection requirements implemented to assist the State Agency in the administration of those programs.
- C. The State Agency will use the SSA data governed by this Agreement to determine entitlement and eligibility of individuals for one or more of the following programs, which are specifically identified in the IEA:
  1. Temporary Assistance to Needy Families (TANF) program under Part A of Title IV of the Act;
  2. Medicaid provided under an approved State plan or an approved waiver under Title XIX of the Act;
  3. State Children's Health Insurance Program (CHIP) under Title XXI of the Act, as amended by the Children's Health Insurance Program Reauthorization Act of 2009;

4. Supplemental Nutritional Assistance Program (SNAP) under the Food Stamp Act of 1977 (7 U.S.C. § 2011, et seq.);
  5. Women, Infants and Children Program (WIC) under the Child Nutrition Act of 1966 (42 U.S.C. § 1771, et seq.);
  6. Medicare Savings Programs (MSP) under 42 U.S.C. § 1396a(10)(E);
  7. Unemployment Compensation programs provided under a state law described in section 3304 of the Internal Revenue Code of 1954;
  8. Low Income Heating and Energy Assistance (LIHEAP or home energy grants) program under 42 U.S.C. § 8621;
  9. State-administered supplementary payments of the type described in section 1616(a) of the Act;
  10. Programs under a plan approved under Titles I, X, XIV, or XVI of the Act;
  11. Foster Care and Adoption Assistance under Title IV of the Act;
  12. Child Support Enforcement programs under section 453 of the Act (42 U.S.C. § 653);
  13. Other applicable federally funded programs administered by the State Agency under Titles I, IV, X, XIV, XVI, XVIII, XIX, XX, and XXI of the Act; and
  14. Any other federally funded programs administered by the State Agency that are compatible with SSA's programs.
- D. The State Agency will ensure that SSA data disclosed for the specific purpose of administering a particular federally funded benefit program is used only to administer that program.

### III. Justification and Expected Results

#### A. Justification

This Agreement and related data exchanges with the State Agency are necessary for SSA to assist the State Agency in its administration of federally funded benefit programs by providing the data required to accurately determine entitlement and eligibility of individuals for benefits provided under these programs. SSA uses computer technology to transfer the data because it is more economical, efficient, and faster than using manual processes.

#### B. Expected Results

The State Agency will use the data provided by SSA to improve public service and program efficiency and integrity. The use of SSA data expedites the application process and ensures that benefits are awarded only to applicants that satisfy the State Agency's program criteria. A cost-benefit analysis for the exchange made under this Agreement is not required in accordance with the determination by the SSA Data Integrity Board (DIB) to waive such analysis pursuant to 5 U.S.C. § 552a(u)(4)(B).

#### **IV. Record Description**

##### **A. Systems of Records (SOR)**

SSA SORs used for purposes of the subject data exchanges include:

- 60-0058 -- Master Files of SSN Holders and SSN Applications;
- 60-0059 -- Earnings Recording and Self-Employment Income System;
- 60-0090 -- Master Beneficiary Record;
- 60-0103 -- Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB);
- 60-0269 -- Prisoner Update Processing System (PUPS); and
- 60-0321 -- Medicare Part D and Part D Subsidy File.

The State Agency will only use the tax return data contained in SOR 60-0059 (Earnings Recording and Self-Employment Income System) in accordance with 26 U.S.C. § 6103.

##### **B. Data Elements**

Data elements disclosed in computer matching governed by this Agreement are Personally Identifiable Information (PII) from specified SSA SORs, including names, SSNs, addresses, amounts, and other information related to SSA benefits and earnings information. Specific listings of data elements are available at:

<http://www.ssa.gov/dataexchange/>

##### **C. Number of Records Involved**

The maximum number of records involved in this matching activity is the number of records maintained in SSA's SORs listed above in Section IV.A.

#### **V. Notice and Opportunity to Contest Procedures**

##### **A. Notice to Applicants**

The State Agency will notify all individuals who apply for federally funded, state-administered benefits that any data they provide are subject to verification through computer matching with SSA. The State Agency and SSA will provide such notice through appropriate language printed on application forms or separate handouts.

**B. Notice to Beneficiaries/Recipients/Annuitants**

The State Agency will provide notice to beneficiaries, recipients, and annuitants under the programs covered by this Agreement informing them of ongoing computer matching with SSA. SSA will provide such notice through publication in the Federal Register and periodic mailings to all beneficiaries, recipients, and annuitants describing SSA's matching activities.

**C. Opportunity to Contest**

The State Agency will not terminate, suspend, reduce, deny, or take other adverse action against an applicant for or recipient of federally funded, state-administered benefits based on data disclosed by SSA from its SORs until the individual is notified in writing of the potential adverse action and provided an opportunity to contest the planned action. "Adverse action" means any action that results in a termination, suspension, reduction, or final denial of eligibility, payment, or benefit. Such notices will:

1. Inform the individual of the match findings and the opportunity to contest these findings;
2. Give the individual until the expiration of any time period established for the relevant program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond; and
3. Clearly state that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the SSA data are correct and will effectuate the planned action or otherwise make the necessary adjustment to the individual's benefit or entitlement.

**VI. Records Accuracy Assessment and Verification Procedures**

Pursuant to 5 U.S.C. § 552a(p)(1)(A)(ii), SSA's DIB has determined that the State Agency may use SSA's benefit data without independent verification. SSA has independently assessed the accuracy of its benefits data to be more than 99 percent accurate when the benefit record is created.

Prisoner and death data, some of which is not independently verified by SSA, does not have the same degree of accuracy as SSA's benefit data. Therefore, the State Agency must independently verify these data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

Based on SSA's Office of Quality Review "Fiscal Year 2014 Enumeration Accuracy Report," the SSA Enumeration System database (the Master Files of SSN Holders and SSN Applications System) used for SSN matching is 99 percent accurate for records updated by SSA employees.

Individuals applying for SSNs report their citizenship status at the time they apply for their SSNs. There is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files for a Social Security benefit. The State Agency must independently verify citizenship data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

## **VII. Disposition and Records Retention of Matched Items**

- A. The State Agency will retain all data received from SSA to administer programs governed by this Agreement only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.
- B. The State Agency may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing the State Agency's retention of records.
- C. The State Agency may use any accretions, deletions, or changes to the SSA data governed by this Agreement to update their master files of federally funded, state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing the State Agency's retention of records.
- D. The State Agency may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this Agreement.
- E. SSA will delete electronic data input files received from the State Agency after it processes the applicable match. SSA will retire its data in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

## **VIII. Security Procedures**

SSA and the State Agency will comply with the security and safeguarding requirements of the Privacy Act, as amended by the CMPPA, related OMB guidelines, FISMA, related NIST guidelines, and the current revision of Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, available at <http://www.irs.gov>. In addition, SSA

and the State Agency will have in place administrative, technical, and physical safeguards for the matched data and results of such matches. Additional administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency, including SSA's *Electronic Information Exchange Security Requirements and Procedures for State and local Agencies Exchanging Electronic Information with SSA*, as well as specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

SSA has the right to monitor the State Agency's compliance with FISMA, the terms of this Agreement, and the IEA and to make onsite inspections of the State Agency for purposes of auditing compliance, if necessary, during the lifetime of this Agreement or of any extension of this Agreement. This right includes onsite inspection of any entity that receives SSA information from the State Agency under the terms of this Agreement, if SSA determines it is necessary.

#### **IX. Records Usage, Duplication, and Redisclosure Restrictions**

- A. The State Agency will use and access SSA data and the records created using that data only for the purpose of verifying eligibility for the specific federally funded benefit programs identified in the IEA.**
- B. The State Agency will comply with the following limitations on use, duplication, and redisclosure of SSA data:**
  - 1. The State Agency will not use or redisclose the data disclosed by SSA for any purpose other than to determine eligibility for, or the amount of, benefits under the state-administered income/health maintenance programs identified in this Agreement.**
  - 2. The State Agency will not extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs identified in this Agreement. In limited circumstances that are approved by SSA, the State Agency may extract information about an individual other than the applicant/recipient when the applicant/recipient has provided identifying information about the individual and the individual's income or resources affect the applicant's/recipient's eligibility for such program.**
  - 3. The State Agency will not disclose to an applicant/recipient information about another individual (i.e., an applicant's household member) without the written consent from the individual to whom the information pertains.**
  - 4. The State Agency will use the Federal tax information (FTI) disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to section 1137 programs and child support enforcement**



programs in accordance with 26 U.S.C. § 6103(l)(7) and (8). The State Agency receiving FTI will maintain all FTI from IRS in accordance with 26 U.S.C. § 6103(p)(4) and the IRS Publication 1075. Contractors and agents acting on behalf of the State Agency will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103 and the current revision IRS Publication 1075.

5. The State Agency will use the citizenship status data disclosed by SSA only to determine entitlement of new applicants to: (a) the Medicaid program and CHIP pursuant to CHIPRA, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA. The State Agency will further comply with additional terms and conditions regarding use of citizenship data, as set forth in the State Agency's IEA.
6. The State Agency will restrict access to the data disclosed by SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with the purposes identified in this Agreement.
7. The State Agency will enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties whereby such contractor or agent agrees to abide by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement. The State Agency will provide its contractors and agents with copies of this Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing this Agreement, and thereafter at SSA's request, the State Agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.
8. If the State Agency is authorized or required – pursuant to an applicable law, regulation, or intra-governmental documentation – to provide SSA data to another State or local government entity for the administration of the federally funded, state-administered programs covered by this Agreement, the State Agency must ensure that the State or local government entity, including its employees, abides by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement and the IEA. At SSA's request, the State Agency will provide copies of any applicable law, regulation, or intra-governmental documentation that authorizes the intra-governmental relationship with the State or local government entity. Upon request from SSA, the State Agency will also establish how it ensures that State or local government entity complies with the terms of this Agreement and the IEA.
9. The State Agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this Agreement



may be subject to civil and criminal sanctions pursuant to applicable Federal statutes.

10. The State Agency will conduct triennial compliance reviews of its contractor(s) and agent(s) no later than three years after the initial approval of the security certification to SSA. The State Agency will share documentation of its recurring compliance reviews with its contractor(s) and agent(s) with SSA. The State Agency will provide documentation to SSA during its scheduled compliance and certification reviews or upon request.

C. The State Agency will not duplicate in a separate file or disseminate, without prior written permission from SSA, the data governed by this Agreement for any purpose other than to determine entitlement to, or eligibility for, federally funded benefits. The State Agency proposing the redisclosure must specify in writing to SSA what data are being disclosed, to whom, and the reasons that justify the redisclosure. SSA will not give permission for such redisclosure unless the redisclosure is required by law or essential to the conduct of the matching program and authorized under a routine use. To the extent SSA approves the requested redisclosure, the State Agency will ensure that any entity receiving the redisclosed data will comply with the procedures and limitations on use, duplication, and redisclosure of SSA data, as well as all administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency including specific guidance on safeguarding and reporting responsibilities for PII, as set forth in this Agreement and the accompanying IEAs.

#### **X. Comptroller General Access**

The Comptroller General (the Government Accountability Office) may have access to all records of the State Agency that the Comptroller General deems necessary to monitor and verify compliance with this Agreement in accordance with 5 U.S.C. § 552a(o)(1)(K).

#### **XI. Duration, Modification, and Termination of the Agreement**

##### **A. Duration**

1. This Agreement is effective from July 1, 2017 (Effective Date) through December 31, 2018 (Expiration Date).
2. In accordance with the CMPPA, SSA will: (a) publish a Computer Matching Notice in the Federal Register at least 30 days prior to the Effective Date; (b) send required notices to the Congressional committees of jurisdiction under 5 U.S.C. § 552a(o)(2)(A)(i) at least 40 days prior to the

Effective Date; and (c) send the required report to OMB at least 40 days prior to the Effective Date.

3. Within 3 months prior the Expiration Date, the SSA DIB may, without additional review, renew this Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:
  - the applicable data exchange will continue without any change; and
  - SSA and the State Agency certify to the DIB in writing that the applicable data exchange has been conducted in compliance with this Agreement.
4. If either SSA or the State Agency does not wish to renew this Agreement, it must notify the other party of its intent not to renew at least 3 months prior to the Expiration Date.

#### B. Modification

Any modification to this Agreement must be in writing, signed by both parties, and approved by the SSA DIB.

#### C. Termination

The parties may terminate this Agreement at any time upon mutual written consent of both parties. Either party may unilaterally terminate this Agreement upon 90 days advance written notice to the other party; such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow or terminate this Agreement if SSA determines, in its sole discretion, that the State Agency has violated or failed to comply with this Agreement.

### XII. Reimbursement

In accordance with section 1106(b) of the Act, the Commissioner of SSA has determined not to charge the State Agency the costs of furnishing the electronic data from the SSA SORs under this Agreement.

### XIII. Disclaimer

SSA is not liable for any damages or loss resulting from errors in the data provided to the State Agency under any IEAs governed by this Agreement. Furthermore, SSA

is not liable for any damages or loss resulting from the destruction of any materials or data provided by the State Agency.

The performance or delivery by SSA of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with proper performance of the official duties and obligations of SSA and the relative importance of this request to others. If for any reason SSA delays or fails to provide services, or discontinues the services or any part thereof, SSA is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

#### **XIV. Points of Contact**

##### **A. SSA Point of Contact**

###### **San Francisco Regional Office:**

Jamie Lucero, Director

San Francisco Regional Office, Center for Disability and Programs Support

1221 Nevin Ave., 6<sup>th</sup> Floor

Richmond, CA 94801

Phone: 510-970-8297

Fax: 510-970-8101

Email: [Jamie.Lucero@ssa.gov](mailto:Jamie.Lucero@ssa.gov)

##### **B. State Agency Point of Contact**

Sonia Herrera

California Health and Human Services Agency

1600 Ninth Street

Sacramento, CA 95814

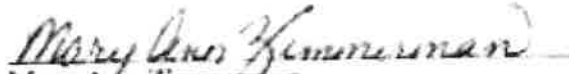
Phone: 916-654-3459 / Fax: 916-440-5001

Email: [Sonia.Herrera@chhs.ca.gov](mailto:Sonia.Herrera@chhs.ca.gov)


**XV. SSA and Data Integrity Board Approval of Model CMPPA Agreement**

The signatories below warrant and represent that they have the competent authority on behalf of SSA to approve the model of this CMPPA Agreement.

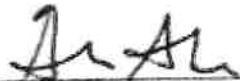
**SOCIAL SECURITY ADMINISTRATION**



Mary Ann Zimmerman  
Acting Deputy Executive Director  
Office of Privacy and Disclosure  
Office of the General Counsel

  
Date

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



Glenn Sklar  
Acting Chair  
SSA Data Integrity Board

  
Date

**XVI. Authorized Signatures**

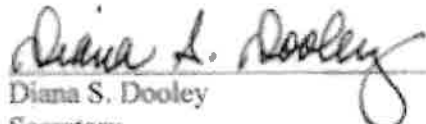
The signatories below warrant and represent that they have the competent authority on behalf of their respective agency to enter into the obligations set forth in this Agreement.

**SOCIAL SECURITY ADMINISTRATION**

  
\_\_\_\_\_  
Grace M. Kim  
Regional Commissioner  
San Francisco

6/2/17  
\_\_\_\_\_  
Date

**HEALTH AND HUMAN SERVICES AGENCY**

  
\_\_\_\_\_  
Diana S. Dooley  
Secretary

May 24, 2017  
\_\_\_\_\_  
Date

**ATTACHMENT 2**

**AUTHORIZED DATA EXCHANGE SYSTEM(S)**

**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:

<b>SVES I:</b>	This batch provides strictly SSN verification.
<b>SVES I/Citizenship*</b>	This batch provides strictly SSN verification and citizenship data.
<b>SVES II:</b>	This batch provides strictly SSN verification and MBR benefit information
<b>SVES III:</b>	This batch provides strictly SSN verification and SSR/SVB.
<b>SVES IV:</b>	This batch provides SSN verification, MBR benefit information, and SSR/SVB information, which represents all available SVES data.

*\* Citizenship status data disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3 is only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants.*





**ATTACHMENT 3**

**SYSTEM SECURITY REQUIREMENTS THROUGH THE ICON SYSTEM**

Not Applicable

**Attachment 3**

---

**Systems Security Requirements for SWA Access  
to SSA Information Through the ICON System**

---

12/9/2016

## **Systems Security Requirements for SWA Access to SSA Information Through the ICON System**

### **A. General Systems Security Standards**

SWA's that request and receive information from SSA through the ICON system must comply with the following general systems security standards concerning access to and control of SSA information. The SWA must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information retrieved from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The SWA must employ both physical and electronic safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and State laws. SSA may, at its discretion, make on-site inspections or other provisions to ensure that adequate safeguards are being maintained by the SWA.

### **B. System Security Requirements for SWA's**

SWA's that receive SSA information through the ICON system must comply with the following systems security requirements which must be met before DOL will approve a request from an SWA for online access to SSA information through the ICON system. The SWA system security design and procedures must conform to these requirements. They must be documented by the SWA and subsequently certified by either DOL or by an Independent Verification and Validation (IV&V) contractor prior to initiating transactions to and from SSA through the ICON.

No specific format for submitting this documentation to DOL is required. However, regardless of how it is presented, the information should be submitted to DOL in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the SWA. Written documentation should address each of the following security control areas:

## **1. General System Security Design and Operating Environment**

The SWA must provide a written description of its' system configuration and security features. This should include the following:

- a. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and
- b. A description of how SSA information will be obtained by and presented to SWA users, including sample computer screen presentation formats and an explanation of whether the SWA system will request information from SSA by means of systems generated or user initiated transactions; and
- c. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the SWA system and an explanation of their job descriptions.

### ***Meeting this Requirement***

SWA's must explain in their documentation the overall design and security features of their system. During onsite certification, the IV&V contractor, or other certifier, will use the SWA's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and for verifying that the SWA systems and procedures conform to SSA requirements.

Following submission to the DOL in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

## **2. Automated Audit Trail**

SWA's receiving SSA information through the ICON system must implement and maintain a fully automated audit trail system capable of data collection, data retrieval and data storage. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator and relevant business purpose (i.e. the SWA client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored

## Exhibit F, Attachment B

in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a “need to know” and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before DOL will approve the SWA’s request for access to SSA information through the ICON system.

If SSA-supplied information is retained in the SWA system, or if certain data elements within the SWA system will indicate to users that the information has been verified by SSA, the SWA system also must capture an audit trail record of any user who views SSA information stored within the SWA system. The audit trail requirements for these inquiry transactions are the same as those outlined above for SWA transactions requesting information directly from SSA.

### ***Meeting this Requirement***

The SWA must include in their documentation a description of their audit trail capability and a discussion of how it conforms to SSA’s requirements. During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the system’s audit trail and retrieval capability. The SWA must be able to identify employee’s who initiate online requests for SSA information (or, for systems generated transaction designs, the SWA case that triggered the transaction), the time and date of the request, and the purpose for which the transaction was originated. The certifier, or IV&V contractor, also will request a demonstration of the system’s audit trail capability for tracking the activity of SWA employees that are permitted to view SSA supplied information within the SWA system, if applicable.

During its future compliance reviews (see below), the SSA also will test the SWA audit trail capability by requesting verification of a sample of transactions it has processed from the SWA after implementation of access to SSA information through the ICON system.

### **3. System Access Control**

The SWA must utilize and maintain technological (logical) access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The SWA must use a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user’s system identification code. The SWA must have

## Exhibit F, Attachment B

management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the SWA system.

### ***Meeting this Requirement***

The SWA must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the function responsible for PIN/password issuance and maintenance.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions to verify their responsibilities in the SWA's access control process and will observe a demonstration of the procedures for logging onto the SWA system and for accessing SSA information.

### **4. Monitoring and Anomaly Detection**

The SWA's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to an SWA client case (e.g. celebrities, SWA employees, relatives, etc.) If the SWA system design is transaction driven (i.e. employees cannot initiate transactions themselves, rather, the SWA system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an SWA employee unless the SWA system contains a record containing the client's Social Security Number), then the SWA needs only minimal additional monitoring and anomaly detection. If such designs are used, the SWA only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the SWA system by employees not authorized to have access to such information.

If the SWA design does not include either of the security control features described above, then the SWA must develop and implement compensating security controls to prevent their employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of queries requested by individual SWA employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The SWA system must produce reports providing SWA management and/or supervisors with the capability to appropriately monitor user activity, such as:

## Exhibit F, Attachment B

- User ID exception reports

This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password.

- Inquiry match exception reports

This type of report captures information about users who may be initiating transactions for Social Security Numbers that have no client case association within the SWA system.

- System error exception reports

This type of report captures information about users who may not understand or be following proper procedures for access to SSA information through the ICON system.

- Inquiry activity statistical reports

This type of report captures information about transaction usage patterns among authorized users, which would provide SWA management a tool for monitoring typical usage patterns compared to extraordinary usage.

The SWA must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors, or to local security officers, to ensure that the reports are used by those whose responsibilities include monitoring the work of the authorized users.

### ***Meeting this Requirement***

The SWA must explain in their documentation how their system design will monitor and/or prevent their employees from browsing SSA information. If the design is based on a "permission module" (see above), a similar design, or is transaction driven (i.e. no employee initiated transactions) then the SWA does not need to implement additional systematic and/or managerial oversight procedures to monitor their employees access to SSA information. The SWA only needs to monitor user access control violations. The documentation should clearly explain how the system design will prevent SWA employees from browsing SSA records.

If the SWA system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an SWA client), then the SWA must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA

## Exhibit F, Attachment B

information. The SWA should include sample report formats demonstrating their capability to produce the types of reports described above, and the SWA should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the SWA's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the SWA will demonstrate how the system triggers requests for information from SSA.
- If the design is based on a permission module, the SWA will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the SWA system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the SWA system.)
- If the design is based on systematic and/or managerial monitoring and oversight, the SWA will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification, the IV&V contractor, or other certifier, also will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

### **5. Management Oversight and Quality Assurance**

The SWA must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information through the ICON system, and to ensure there is ongoing compliance with the terms of the SWA's data exchange agreement with SSA. The management oversight function must consist of one or more SWA management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to



determine whether the requests comply with these guidelines. These functions should be performed by SWA employees whose job functions are separate from those who request or use information from SSA.

***Meeting this Requirement***

The SWA must document that they will establish and/or maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information, and oversight and monitoring of the use of SSA information within the SWA business process. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

**6. Security Awareness and Employee Sanctions**

The SWA must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other Federal and State laws governing use and misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

***Meeting this Requirement***

The SWA must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The SWA should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The IV&V contractor, or other certifier, also will meet with a sample of SWA employees to assess their level of training and

## Exhibit F, Attachment B

understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

### **7. Data and Communications Security**

The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

#### **D. Onsite Systems Security Certification Review**

The SWA must obtain and participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the ICON system. DOL will require an initial onsite systems security certification review to be performed by either an independent IV&V contractor, or other DOL approved certifier. The onsite certification will address each of the requirements described above and will include, where appropriate, a demonstration of the SWA's implementation of each requirement. The review will include a walkthrough of the SWA's data center to observe and document physical security safeguards, a demonstration of the SWA's implementation of online access to SSA information through the ICON system, and discussions with managers/supervisors. The IV&V contractor, or other certifier, also will visit at least one of the SWA's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.

The IV&V contractor, or other certifier, will separately document and certify SWA compliance with each SSA security requirement. To fully comply with SSA's security requirements and be certified to connect to SSA through the ICON system, the SWA must submit to DOL a complete package of documentation as described above and a complete certification from an independent IV&V contractor, or other DOL approved certifier, that the SWA system design and infrastructure is in agreement with the SWA documentation and consistent with SSA requirements. Any unresolved or unimplemented security control features must be resolved by the SWA before DOL will authorize their connection to SSA through the ICON system.

Following initial certification and authorization from DOL to connect to SSA through the ICON system, SSA is responsible for future systems security compliance reviews. SSA conducts such reviews approximately once every three years, or as needed if there is a significant change in the SWA's computing platform, or if there is a violation of any of SSA's systems security requirements or an unauthorized disclosure of SSA information by the SWA. The format of those reviews generally consists of

## Exhibit F, Attachment B

reviewing and updating the SWA compliance with the systems security requirements described above.

Exhibit F, Attachment B

SENSITIVE DOCUMENT

**ATTACHMENT 4**

**ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS  
AND PROCEDURES**

(Technical Systems Security Requirements- TSSR)

Attachment 4 is a sensitive document, not a public document, and shall not in any manner be made available to the public without prior approval from DHCS.



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

**SENSITIVE DOCUMENT**

**Version 7.0  
July 2015**

## TABLE OF CONTENTS

1. **Introduction**
2. **Electronic Information Exchange (EIE) Definition**
3. **Roles and Responsibilities**
4. **General Systems Security Standards**
5. **Systems Security Requirements**
  - 5.1 **Overview**
  - 5.2 **General System Security Design and Operating Environment**
  - 5.3 **System Access Control**
  - 5.4 **Automated Audit Trail**
  - 5.5 **Personally Identifiable Information (PII)**
  - 5.6 **Monitoring and Anomaly Detection**
  - 5.7 **Management Oversight and Quality Assurance**
  - 5.8 **Data and Communications Security**
  - 5.9 **Incident Reporting**
  - 5.10 **Security Awareness and Employee Sanctions**
  - 5.11 **Contractors of Electronic Information Exchange Partners**
  - 5.12 **Cloud Service Providers (CSP) for Electronic Information Exchange Partners**
6. **Security Certification and Compliance Review Programs**
  - 6.1 **The Security Certification Program**
  - 6.2 **Documenting Security Controls in the Security Design Plan (SDP)**
    - 6.2.1 **When the SDP is Required**
  - 6.3 **The Certification Process**
  - 6.4 **The Compliance Review Program and Process**
    - 6.5.1 **EIEP Compliance Review Participation**
  - 6.6 **Scheduling the Onsite Review**
7. **Additional Definitions**
8. **Regulatory References**
9. **Frequently Asked Questions**

## 1. Introduction

Federal standards require the Social Security Administration (SSA) to maintain oversight of the information it provides to its **Electronic Information Exchange Partners (EIEPs)**. EIEPs must protect the information with efficient and effective security controls. EIEPs are entities that have electronic information exchange agreements with the agency.

This document consistently references the concept of **Electronic Information Exchange Partners (EIEP)**; however, our **Compliance Review Questionnaire (CRQ)** and **Security Design Plan (SDP)** documents will use the terms “state agency” or “state agency, contractor(s), and agent(s)” for clarity. Most state officials and agreement signatories are not familiar with the acronym EIEP; therefore, SSA will continue to use the terms “state agency” or “state agency, contractor(s), and agent(s)” in the same manner as the Computer Matching and Privacy Protection Act (CMPPA) and Information Exchange Agreements (IEA). This allows for easier alignment and mapping back to our data exchange agreements between state agencies and SSA. It will also provide a more “user-friendly” experience for the state officials who complete these forms on behalf of their state agencies.

The objective of this document is twofold. The first is to ensure that SSA can properly certify EIEPs as compliant with SSA security standards, requirements, and procedures. The second is to ensure that EIEPs adequately safeguard electronic information provided to them by SSA.

This document helps EIEPs understand the criteria that SSA uses when evaluating and certifying the system design and security features used for electronic access to SSA-provided information. Finally, this document provides the framework and general procedures for SSA’s Security Certification and Compliance Review Programs.

The primary statutory authority that supports the information contained in this document is the **Federal Information Security Management Act (FISMA)**. FISMA became law as part of the **Electronic Government Act of 2002**. FISMA is the United States legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or manufactured threats. FISMA assigned the **National Institute of Standards and Technology (NIST)**, a branch of the U.S. Department of Commerce, the responsibility to outline and define compliance with FISMA. Unless otherwise stated, all of SSA’s requirements mirror the NIST-defined management, operational, and technical controls listed in the various NIST Special Publications (SP) libraries of technical guidance documents.

To gain electronic access to SSA-provided information, under the auspices of a data exchange agreement, EIEP’s must comply with SSA’s most current **Technical System Security Requirements** (hereafter referred to as **TSSRs**) to gain access to SSA-provided information. This document is synonymous with the **Electronic Information Exchange Security Requirements and Procedures for State and**

**Local Agencies Exchanging Electronic Information with the Social Security Administration** in the agreements. The TSSR specifies minimally acceptable levels of security standards and controls to protect SSA-provided information. SSA maintains the TSSR as a living document—subject to change—that addresses emerging threats, new attack methods and the development of new technology that potentially places SSA-provided information at risk. EIEPs may proactively ensure their ongoing compliance to the TSSR by periodically requesting the most current version from SSA. SSA will work with EIEPs to resolve deficiencies, which result from updates to the TSSRs. SSA refers to this process as **Gap Analysis**. EIEPs may proactively ensure their ongoing compliance with the TSSRs by periodically requesting the most current TSSR package from their SSA Point of Contact (POC) from the data exchange agreement.

SSA's standard for categorization of information (Moderate) and information systems is to provide appropriate levels of security according to risk level. Additions, deletions, or modification of security controls directly affect the level of security and due diligence SSA requires EIEPs use to mitigate risks. The emergence of new threats, attack methods, and the development of new technology warrants frequent reviews and revisions to our TSSR. Consequently, EIEPs should expect SSA's TSSR to evolve in harmony with the industry.

## 2. Electronic Information Exchange (EIE) Definition

For discussion purposes herein, EIE is any electronic process in which SSA discloses information under its control to any third party for program or non-program purposes, without the specific consent of the subject individual or any agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the programmatic systems of parties to electronic information sharing agreements with SSA. This includes direct terminal access (DTA) to SSA systems, batch processing, and variations thereof (e.g., online query) regardless of the systematic method used to accomplish the activity or to interconnect SSA with the EIEP.

## 3. Roles and Responsibilities

The SSA **Office of Information Security (OIS)** has agency-wide responsibility for interpreting, developing, and implementing security policy; providing security and integrity review requirements for all major SSA systems; managing SSA's fraud monitoring and reporting activities, developing and disseminating security training and awareness materials, and providing consultation and support for a variety of agency initiatives. SSA's security reviews ensure that external systems receiving information from SSA are secure and operate in a manner consistent with SSA's Information Technology (IT) security policies and in compliance with the terms of electronic data exchange agreements executed by SSA with outside entities. Within the context of SSA's security policies and the terms of the electronic data exchange



## Exhibit F, Attachment B

agreements with SSA's EIEPs, SSA exclusively conducts and brings to closure initial security certifications and triennial security compliance reviews. This includes (but not limited to) any EIEP that processes, maintains, transmits, or stores SSA-provided information in accordance with pertinent Federal requirements.

- a. The SSA Regional **Data Exchange Coordinators** (DECs) serve as a bridge between SSA and EIEPs. DECs assist in coordinating data exchange security review activities with EIEPs; (e.g., providing points of contact with state agencies, assisting in setting up security reviews, etc.) DECs are also the first points of contact for states if an employee of a state agency or an employee of a state agency's contractor or agent becomes aware of suspected or actual loss of SSA-provided information.
- b. SSA requires **EIEPs** to adhere to the standards, requirements, and procedures, published in this TSSR document.
  - "Personally Identifiable Information (PII)," covered under several Federal laws and statutes, refers to specific information about an individual used to trace that individual's identity. Information such as his/her name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records, alone, or when combined with other personal or identifying information is linkable or lined to a specific individual's medical, educational, financial, and employment information.
  - The data (last 4 digits of the SSN) that SSA provides to its EIEPs for purposes of the Help America Vote Act (HAVA) does not identify a specific individual; therefore, is not "PII" as defined by the Act.
  - Both SSA and EIEPs must remain diligent in the responsibility for establishing appropriate management, operational, and technical safeguards to ensure the confidentiality, integrity, and availability of its records and to protect against any anticipated threats or hazards to their security or integrity.
- c. A State Transmission/Transfer Component (STC) is an organization that performs as an electronic information conduit or collection point for one of more other entities (also referred to as a hub). An STC must also adhere to the same management, operational and technical controls as SSA and the EIEP.

***NOTE: Disclosure of Federal Tax Information (FTI) is limited to certain Federal agencies and state programs supported by federal statutes under Sections 1137, 453, and 1106 of the Social Security Act. For information regarding***

***safeguards for protecting FTI, consult IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.***

**4. General Systems Security Standards**

EIEPs that request and receive information electronically from SSA must comply with the following general systems security standards concerning access to and control of SSA-provided information.

***NOTE: EIEPs may not create separate files or records comprised solely of the information provided by SSA.***

1. EIEPs must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA-provided information neither prevents nor impedes the EIEP's ability to:
  - safeguard the information in conformance with SSA requirements
  - efficiently investigate fraud, data breaches, or security events that involve SSA-provided information
  - detect instances of misuse or abuse of SSA-provided information

**For example, Utilization of cloud computing may have the potential to jeopardize an EIEP's compliance with the terms of their agreement or associated systems security requirements and procedures.**

2. The EIEP must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.
3. The EIEP must use the software and/or devices provided to the EIEPs only in support of the current agreement(s) between the EIEPs and SSA.
4. SSA prohibits the EIEP from modifying any software or devices provided to the EIEPs by SSA.
5. EIEPs must ensure that SSA-provided information is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in geographic or virtual areas not subject to U.S. law.
6. EIEPs must restrict access to the information to authorized users who need it to perform their official duties.

***NOTE: Contractors and agents (hereafter referred to as contractors) of the EIEP who process, maintain, transmit, or store SSA-provided information are held to the same security requirements as employees of the EIEP. Refer to the section 'Contractors of Electronic Information Exchange Partners in the Systems Security Requirements' for additional information.***

7. EIEPs must store information received from SSA in a manner that, at all times, is

## Exhibit F, Attachment B

physically and electronically secure from access by unauthorized persons.

8. The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel.
9. EIEPs must employ both physical and technological barriers to prevent unauthorized retrieval of SSA-provided information via computer, remote terminal, or other means.
10. EIEPs must have formal PII incident response procedures. When faced with a security incident, caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA-provided information affected by the incident.
11. EIEPs must have an active and robust security awareness program, which is mandatory for all employees who access SSA-provided information.
12. EIEPs must advise employees with access to SSA-provided information of the confidential nature of the information, the safeguards required to protecting the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and state laws.
13. In accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) on Contingency Planning requirements and recommendations, SSA requires EIEPs to document a senior management approved Contingency plan that includes a disaster recovery plan that addresses both natural disaster and cyber-attack situations.
14. SSA requires the Contingency Plan to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that address the security of SSA-provided information if a disaster occurs.
15. At its discretion, SSA or its designee must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

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

## 5. Systems Security Requirements

### 5.1 Overview

SSA's TSSR represent the current industry standard for security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations, statutes, standards, and guidelines. Additionally, SSA's TSSR includes organizationally defined interpretations, policies, and procedures mandated by the authority of the Commissioner of Social Security in areas when or where other cited authorities may be silent or non-specific.

SSA must certify that the EIEP has implemented security controls that meet the requirements and work as intended, before the authorization to initiate transactions to and from SSA, through batch data exchange processes or online processes such as State Online Query (SOLQ) or Internet SOLQ (SOLQ-I).

The TSSR address management, operational, and technical controls regarding security safeguards to ensure only authorized disclosure and usage of SSA provided information used, maintained, transmitted, or stored by SSA's EIEPs. SSA requires EIEPs to maintain an organizational access control structure that adheres to a three-tiered best practices model. The SSA recommended model is "separation of duties," "need-to-know" and "least privilege."

SSA requires EIEPs to document and notify SSA prior to sharing SSA-provided information with another state entity, or to allow them direct access to their system. **This includes (but not limited to) law enforcement, other state agencies, and state organizations that perform audit, quality, or integrity functions.**

SSA recommends that the EIEP develop and publish a comprehensive Information Technology (IT) Systems Security Policy document that specifically addresses:

- 1) the classification of information processed and stored within the network,
- 2) management, operational, and technical controls to protect the information stored and processed within the network,
- 3) access to the various systems and subsystems within the network,
- 4) Security Awareness Training,

**Exhibit F, Attachment B**

- 5) Employee and End User Sanctions Policy,
- 6) Contingency Planning and Disaster Recovery
- 7) Incident Response Policy, and
- 8) The disposal of protected information and sensitive documents derived from the system or subsystems on the network.

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

**5.2 General System Security Design and Operating Environment**  
*(Planning (PL) Family – (System Security Plan), Contingency Plan (CP) Family, Physical and Environmental (PE) Family, NIST SP 800-53 rev. 4)*

In accordance with the NIST suite of Special Publications (SP) (e.g., 800-53, 800-34, etc.), SSA requires the EIEP to maintain policies, procedures, descriptions, and explanations of their overall system design, configuration, security features, and operational environment. They should include explanations of how they conform to SSA's TSSRs. The EIEPs General System Security design and Operating Environment must also address:

- a) the operating environment(s) in which the EIEP will utilize, maintain, store, and transmit SSA-provided information,
- b) the business process(es) in which the EIEP will use SSA-provided information,
- c) the physical safeguards employed to ensure that unauthorized personnel, the public or visitors to the agency cannot access SSA-provided information,
- d) details of how the EIEP keeps audit information pertaining to the use and access to SSA-provided information and associated applications readily available,
- e) electronic safeguards, methods, and procedures for protecting the EIEP's network infrastructure and for protecting SSA-provided information while in transit, in use within a process or application, and at rest ,
- f) a senior management approved Information System Contingency Plan (ISCP) that addresses both internal and external threats. SSA requires the ISCP to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that addresses the security of SSA-provided information if a disaster occurs. SSA recommends that state agencies perform disaster exercises at least once annually.,

## Exhibit F, Attachment B

- g) how the EIEP prevents unauthorized retrieval of SSA-provided information by computer, remote terminal, or other means; including descriptions of security software other than access control software (e.g., security patch and anti-malware software installation and maintenance, etc.)
- h) how the configurations of devices (e.g., servers, workstations, portable devices) involving SSA-provided information complies with recognized industry standards (i.e. NIST SP's) and SSA's TSSR, and
- i) organizational structure of the agency, number of users, and all external entities that will have access to the system and/or application that displays, transmits, and/or application that displays, transmits and/or stores SSA-provided information.

Note: At its discretion, SSA or a third party (i.e. contractor) must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

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

### 5.3 System Access Control

(Access Control (AC) Family, *NIST SP 800-53 rev. 4*)

EIEPs must utilize and maintain technological (logical) access controls that limit access to SSA-provided information and associated transactions and functions to only those users, processes acting on behalf of authorized users, or devices (including other information systems) authorized for such access based on their official duties or purpose(s). EIEPs must employ a recognized user-access security software package (e.g., RAC-F, ACF-2, TOP SECRET, Active Directory, etc.) or a security software design, which is equivalent to such products. The access control software must employ and enforce (1) PIN/password, and/or (2) PIN/biometric identifier, and/or (3) SmartCard/biometric identifier, etc., (for authenticating users), (and lower case letters, numbers, and special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

The EIEP's password policies must require stringent password construction as supported by current NIST guidelines for the user accounts of persons, processes, or devices whose functions require access privileges above those of ordinary users. **SSA strongly recommends Two-Factor Authentication.**

The EIEP's implementation of the control software must comply with recognized industry standards. Password policies should enforce sufficient construction strength (length and complexity) to defeat or minimize risk-based identified vulnerabilities and ensure limitations for password repetition. Technical controls should enforce periodic password changes based on a risk-based standard (e.g., maximum password age of 90 days, minimum password age of 3 – 7 days) and enforce automatic disabling of user accounts that have been inactive for a specified period of time (e.g., 90 days).

The EIEP's password policies must require stringent password construction (e.g., passwords greater than eight characters in length requiring upper and lower case letters, numbers, and/or special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.



## Exhibit F, Attachment B

In addition, SSA has the following specific requirements in the area of Access Control:

1. Upon hiring or before granting access to SSA-provided information, EIEPs should verify the identities of any employees, contractors, and agents who will have access to SSA-provided information in accordance with the applicable agency or state's "personnel identity verification policy."
2. SSA requires that state agencies have a logical control feature that designates a maximum number of unsuccessful login attempts for agency workstations and devices that store or process SSA-provided information, in accordance with NIST guidelines. SSA recommends no fewer than three (3) and no greater than five (5)..
3. SSA requires that the state agency designate specific official(s) or functional component(s) to issue PINs, passwords, biometric identifiers, or Personal Identity Verification (PIV) credentials to individuals who will access SSA-provided information. **SSA also requires that the state agency prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job-function or category of access.**
4. SSA requires that EIEPs grant access to SSA-provided information based on least privilege, need-to-know, and separation of duties. State agencies should not routinely grant employees, contractors, or agents access privileges that exceed the organization's business needs. SSA also requires that EIEPs periodically review employees, contractors, and agent's system access to determine if the same levels and types of access remain applicable.
5. If an EIEP employee, contractor, or agent is subject to an adverse administrative action by the EIEP (e.g., reduction in pay, disciplinary action, termination of employment), SSA recommends the EIEP remove his or her access to SSA-provided information in advance of the adverse action to reduce the possibility that will the employee will perform unauthorized activities that involve SSA-provided information.

## Exhibit F, Attachment B

6. SSA requires that work-at-home, remote access, and/or Internet access comply with applicable Federal and state security policy and standards. Furthermore, the EIEPs access control policy must define the safeguards in place to adequately protect SSA-provided information for work-at-home, remote access, and/or Internet access.
7. SSA requires EIEPs to design their system with logical control(s) that prevent unauthorized browsing of SSA-provided information. SSA refers to this setup as a **Permission Module**. The term “**Permission Module**” supports a business rule and systematic control that prevents users from browsing a system that contains SSA-provided information. It also supports the principle of **referential integrity**. It should prevent non-business related or unofficial access to SSA-provided information. Before a user or process requests SSA-provided information for verification, the system should verify it is an authorized transaction. Some organizations use the term “referential integrity” to describe the verification step. A properly configured Permission Module should prevent a user from performing any actions not consistent with a need-to-know business process. If a logical permission module configuration is not possible, the state agency must enforce its Access Control List (ACL) in accordance with the principle of least privilege. **The only acceptable compensating control for a system that lacks a permission module is a 100% review of all transactions that involve SSA-provided information.**

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

#### 5.4 Automated Audit Trail

*(Audit and Accountability (AU) Family, NIST SP 800-53 rev. 4)*

SSA requires EIEPs, and other STCs or agencies that provide audit trail services to other state agencies that receive information electronically from SSA, to implement and maintain a fully automated audit trail system (ATS). The system must be capable of creating, storing, protecting, and (efficiently) retrieving and collecting records identifying the individual user who initiates a request for information from SSA or accesses SSA-provided information. At a minimum, individual audit trail records must contain the data needed (including date and time stamps) to associate each query transaction or access to SSA-provided information with its initiator, their action, if any, and the relevant business purpose/process (e.g., SSN verification for Medicaid). Each entry in the audit file must be stored as a separate record, not overlaid by subsequent records. The ATS must create transaction files to capture all input from interactive internet applications that access or query SSA-provided information.

SSA requires that the agency's ATS create an audit record when users view screens that contain SSA-provided information. If an STC handles and audits the EIEP's transactions with SSA, the EIEP is responsible for ensuring that the STC's audit capabilities meet NIST's guidelines for an automated audit trail system. The EIEP must also establish a process to obtain specific audit information from the STC regarding the EIEP's SSA transactions.

SSA requires that EIEPs have automated retrieval and collection of audit records. Such automated functions can be via online queries, automated reports, batch processing, or any other logical means of delivering audit records in an expeditious manner. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request.

Access to the audit file must be restricted to authorized users with a "need to know," audit file data must be unalterable (read-only), and maintained for a minimum of three (3) (preferably seven (7)) years. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request. The EIEP must backup audit trail records on a regular basis to ensure its availability. EIEPs must apply the same level of protection to backup audit files that apply to the original files to ensure the integrity of the data.

## Exhibit F, Attachment B

If the EIEP retains SSA-provided information in a database (e.g., Access database, SharePoint, etc.), or if certain data elements within the EIEP's system indicates to users that SSA verified the information, the EIEP's system must also capture an audit trail record of users who view SSA-provided information stored within the EIEP's system. The retrieval requirements for SSA-provided information at rest and the retrieval requirements for regular transactions are identical. **Similar to the Permission Module requirement above, the only acceptable compensating control for a system that lacks an Automated Audit Trail System (ATS) is a 100% review of all transactions that involve SSA-provided information.**

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

## 5.5 Personally Identifiable Information (PII)

*(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and AP Family – Authority and Purpose (Privacy Controls), NIST SP 800-53 rev. 4)*

**Personally Identifiable Information (PII)** is information used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, alone or when combined with other personal or identifying information linked or linkable to a specific individual. An item such as date and place of birth, mother's maiden name, or father's surname is PII, regardless of whether combined with other data.

SSA defines **a PII loss** as a circumstance when an EIEP employee, contractor, or agent has reason to believe that information on hard copy or in electronic format, which contains PII provided by SSA, left the EIEP's custody or the EIEP disclosed it to an unauthorized individual or entity. PII loss is a reportable incident. SSA requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain SSA-provided information.

If a PII loss involving SSA-provided information occurs or is suspected, the EIEP must be able to quantify the extent of the loss and compile a complete list of the individuals potentially affected by the incident (refer to **Incident Reporting**).

The EIEP should have procedural documents to describe methods and controls for safeguarding SSA-provided PII while in use, at rest, during transmission, or after archiving. The document should explain how the EIEP manages and handles SSA-provided information on print media and explain how the methods and controls conform to NIST requirements. SSA requires that printed items that contain SSA-provided PII always remain in the custody of authorized EIEP employees, contractors, or agents. SSA also requires that the agency destroy the items when no longer required for the EIEP's business process. If retained in paper files for evidentiary purposes, the EIEP should safeguard such PII in a manner that prevents unauthorized personnel from accessing such materials. All agencies that receive SSA-provided information must maintain an inventory of all documents that outline statewide or agency policy and procedures regarding the same.

## 5.6 Monitoring and Anomaly Detection

*(Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-137, E-Government Act of 2002 (P.L. 107-347), and Security Assessment and Authorization (CA) and Risk Assessment (RA) Families, NIST SP 800-53 rev. 4)*

**SSA requires that the EIEPs use an Intrusion Protection System (IPS) or an Intrusion Detection System (IDS).** The EIEP must establish and/or maintain continuous monitoring of its network infrastructure and assets to ensure that:

- 1) the EIEP's security controls continue to be effective over time,
- 2) the EIEP uses industry-standard Security Information Event Manager (SIEM) tools, anti-malware software, and effective antivirus protection,
- 3) only authorized individuals, devices, and processes have access to SSA-provided information,
- 4) the EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions (e.g., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) as soon as they occur,
- 5) the necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes,
- 6) upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk,
- 7) in the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions, and
- 8) trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are readily discernible.

The EIEP's system must include the capability to prevent users from unauthorized browsing of SSA records. SSA requires the use of a transaction-driven **permission module design**, whereby employees are unable to initiate transactions not associated with the normal business process. If the EIEP uses such a design, they also must have anomaly detection to monitor an employee's unauthorized attempts to gain access to SSA-provided information and attempts to obtain information from SSA for clients not in the EIEP's client system. The EIEP should employ measures to ensure the permission module's integrity. Users should not be able to create a bogus case and subsequently delete it in such a manner that it goes undetected. The SSA permission module design employs both role and rules based logical access control restrictions. (Refer to *Access Control*)

If the EIEP's design **does not use** a permission module **and** is not transaction-driven, until at least one of these security features exists, the EIEP must develop and implement **compensating security controls** to deter employees from browsing SSA records. These controls must include monitoring and anomaly detection features, such as: systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of transactions or queries requested or initiated by individuals and include systematic or manual procedures for verifying that requests and queries of SSA-provided information comply with valid official business purposes.

### **Risk Management Program**

**SSA recommends that EIEPs develop and maintain a published Risk Assessment Policy and Procedures document. A Risk Management Program may include, but is not limited to the following:**

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance,
2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls,
3. A function that conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits,
4. An independent function that conducts vulnerability and risk assessments, reviews risk assessment results, and disseminates such information to senior management,
5. A firm commitment from senior management to update the risk assessment whenever there are significant changes to the information

Exhibit F, Attachment B

system or environment of operation or other conditions that may affect the security of SSA-provided information,

6. A robust vulnerability scanning protocol that employs industry standard scanning tools and techniques that facilitate interoperability among tools and automates parts of the vulnerability management process,
7. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk, and
8. Shares information obtained from the vulnerability scanning process and security control assessments with senior management to help eliminate similar vulnerabilities in other information systems that receive, process, transmit, or store SSA-provided information.

**Note: The EIEP's decision to initiate or maintain an official Risk Management Program and establish a formal Risk Assessment Strategy for mitigating risk is strictly voluntary, but highly recommended by SSA.**

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



## 5.7 Management Oversight and Quality Assurance

*(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the AC – Access Control & PM – Program Management Families, NIST SP 800-53 rev. 4)*

SSA requires the EIEP to establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized users have access to SSA-provided information. This will ensure there is ongoing compliance with the terms of the EIEP's electronic information sharing agreement with SSA and the TSSRs established for access to SSA-provided information. The entity responsible for management oversight should consist of one or more of the EIEP's management officials whose job functions include responsibility to ensure that the EIEP only grants access to the appropriate users and position types (least privilege), which require the SSA-provided information to do their jobs (need-to-know).

SSA requires the EIEP to ensure that users granted access to SSA-provided information receive adequate training on the sensitivity of the information, associated safeguards, operating procedures, and the civil and criminal consequences or penalties for misuse or improper disclosure.

SSA requires that EIEPs establish the following job functions and require that only users whose job functions are separate from personnel who request or use SSA-provided information.

### **SSA requires that EIEPs establish the following job functions separate from personnel who request or use SSA-provided information.**

- a) Perform periodic self-reviews to monitor the EIEP's ongoing usage of SSA-provided information.
- b) Perform random sampling of work activity that involves SSA-provided information to determine if the access and usage comply with SSA's requirements

SSA requires the EIEP's system to produce reports that allow management and/or supervisors to monitor user activity. The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

**1. User ID Exception Reports:**

This type of report captures information about users who enter incorrect user IDs when attempting to gain access to the system or to a transaction that initiates requests for information from SSA, including failed attempts to enter a password.

**2. Inquiry Match Exception Reports:**

This type of report captures information about users who initiate transactions for SSNs that have no client case association within the EIEP's system **(the EIEP's management must review 100% of these cases).**

**3. System Error Exception Reports:**

This type of report captures information about users who may not understand or may be violating proper procedures for access to SSA-provided information.

**4. Inquiry Activity Statistical Reports:**

This type of report captures information about transaction usage patterns among authorized users and is a tool that enables the EIEP's management to monitor typical usage patterns in contrast to extraordinary usage patterns.

**The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.**

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

## 5.8 Data and Communications Security

*(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Access Control (AC), Configuration Management (CM), Media Protection (MP), and System and Communication (SC) Families, NIST SP 800-53 rev. 4)*

SSA requires EIEPs to encrypt PII and SSA-provided information when transmitting across dedicated communications circuits between its systems, intrastate communications between its local office locations, and on the EIEP's mobile computers, devices and removable media. The EIEP's encryption methods must align with the Guidelines established by the National Institute of Standards and Technology (NIST). SSA recommends the Advanced Encryption Standard (AES) or Triple DES (Data Encryption Standard 3).

**Files encrypted for external users (when using tools such as Microsoft Word encryption,) require a key length of at least nine characters.** SSA recommends that the key (also referred to as a password) contain both special characters and numbers. SSA supports the NIST Guidelines that requires the EIEP deliver the key so that it does not accompany the media. The EIEP must secure the key when not in use or unattended.

SSA discourages the use of the public Internet for transmission of SSA-provided information. If, however, the EIEP uses the public Internet or other electronic communications, such as emails and faxes to transmit SSA-provided information, they must use a secure encryption protocol such as Secure Socket Layer (SSL) or Transport Layer Security (TLS). SSA also recommends 256-bit encryption protocols or more secure methods such as Virtual Private Network technology. The EIEP should only send data to a secure address or device to which the EIEP can control and limit access to only specifically authorized individuals and/or processes. **SSA recommends that EIEPs use Media Access Control (MAC) Filtering and Firewalls to protect access points from unauthorized devices attempting to connect to the network.**

EIEPs should not retain SSA-provided information any longer than business purpose(s) dictate. The IEA with SSA stipulates a time for data retention. The EIEP should delete, purge, destroy, or return SSA-provided information when the business purpose for retention no longer exists.

The EIEP may not save or create separate files comprised solely of information provided by SSA. The EIEP may apply specific SSA-provided information to the EIEP's matched record from a preexisting data source. Federal law prohibits duplication and redisclosure of SSA-provided information without written approval from SSA.

This prohibition applies to both internal and external sources who do not have a “need-to-know.” SSA recommends that EIEPs use either **Trusted Platform Module (TPM)** or **Hardware Security Module (HSM)** technology solutions to encrypt data at rest on hard drives and other data storage media.

SSA requires EIEPs to prevent unauthorized disclosure of SSA-provided information after they complete processing and after the EIEP no longer requires the information. The EIEP’s operational processes must ensure that no residual SSA-provided information remains on the hard drives of user’s workstations after the user exits the application(s) that use SSA-provided information. If the EIEP must send a computer, hard drive, or other computing or storage device offsite for repair, the EIEP must have a non-disclosure clause in their contract with the vendor. If the EIEP used the item in connection with a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the EIEP’s vendor contract. The EIEP must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the EIEP to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

To sanitize media, the EIEP should use one of the following methods:

1. **Overwriting/Clearing:**

Overwrite utilities can only be used on working devices. Overwriting is appropriate only for devices designed for multiple reads and writes. The EIEP should overwrite disk drives, magnetic tapes, floppy disks, USB flash drives, and other rewriteable media. The overwrite utility must completely overwrite the media. SSA recommends the use of purging media sanitization to make the data irretrievable, protecting data against laboratory attacks or forensics. Reformatting the media does not overwrite the data.

2. **Degaussing:**

Degaussing is a sanitization method for magnetic media (e.g., disk drives, tapes, floppies, etc.). Degaussing is not effective for purging non-magnetic media (e.g., optical discs). SSA and NIST Guidelines require EIEP to use a certified tool designed to degauss each particular type of media. NIST guidelines require certification of the tool to ensure that the magnetic flux applied to the media is strong enough to render the information irretrievable. The degaussing process must render data on the media irretrievable by a laboratory attack or laboratory forensic procedures.

**3. Physical destruction:**

NIST guidelines require physical destruction when degaussing or over-writing cannot be accomplished (for example, CDs, floppies, DVDs, damaged tapes, hard drives, damaged USB flash drives, etc.). Examples of physical destruction include shredding, pulverizing, and burning.

State agencies may retain SSA-provided information in hardcopy only if required to fulfill evidentiary requirements, provided the agencies retire such data in accordance with applicable state laws governing state agency's retention of records. The EIEP must control print media containing SSA-provided information to restrict access to authorized employees who need such access to perform official duties. EIEPs must destroy print media containing SSA-provided information in a secure manner when no longer required for business purposes. SSA requires the EIEP to destroy paper documents that contain SSA-provided information by burning, pulping, shredding, macerating, or other similar means that ensure the information is unrecoverable.

State agencies may use any accretions, deletions, or changes to the SSA-provided information governed by the CMPPA agreement to update their master files or federally funded state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing State Agencies' retention of records.

***NOTE: Hand tearing or lining through documents to obscure information does not meet SSA's requirements for appropriate destruction of PII.***

The EIEP must employ measures to ensure that communications and data furnished to SSA contain no viruses or other malware.

***Special Note regarding Cloud Service Providers:***

If the EIEP will store SSA-provided information through a Cloud Service Provider, please provide the name and address of the cloud provider. Describe the security responsibilities the contract requires to protect SSA-provided information.

SSA will ask for detailed descriptions of the security features contractually required of the cloud provider and information regarding how they will protect SSA-provided information at rest and when in transit.

**EIEPs cannot legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer.**

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

## 5.9 Incident Reporting

*(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Incident Response (IR) Family, NIST SP 800-53 rev. 4)*

FISMA, NIST Guidelines, and Federal Law require the EIEP to develop and implement policies and procedures to respond to potential data breaches or PII losses. EIEPs must articulate, in writing, how the policies and procedures conform to SSA's requirements. The procedures must include the following information:

*If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact **within one hour**, the responsible State Agency official or delegate must report the incident by contacting **SSA's National Network Service Center (NNSC) toll free at 877-697-4889** (select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

If SSA, or another Federal investigating entity (e.g. TIGTA or DOJ), determines that the risk presented by a breach or security incident requires that the state agency notify the subject individuals, the agency must agree to absorb all costs associated with notification and remedial actions connected to security breaches. **SSA and NIST Guidelines encourage agencies to consider establishing incident response teams to address PII and SSA-provided information breaches.**

Incident reporting policies and procedures are part of the security awareness program. Incident reporting pertains to all employees, contractors, or agents regardless as to whether they have direct responsibility for contacting SSA. The written policy and procedures document should include specific names, titles, or functions of the individuals responsible for each stage of the notification process. The document should include detailed instructions for how, and to whom each employee, contractor, or agent should report the potential breach or PII loss.

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

### 5.10 Security Awareness Training and User Sanctions

*(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)*

The EIEP must have an active and robust security awareness program and security training for all employees, contractors, and agents who access SSA-provided information. The training and awareness programs must include:

- a. the sensitivity of SSA-provided information and addresses the Privacy Act and other Federal and state laws governing its use and misuse,
- b. the rules of behavior concerning use and security in systems and/or applications processing SSA-provided information,
- c. the restrictions on viewing and/or copying SSA-provided information,
- d. the responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of SSA-provided information,
- e. the proper disposal of SSA-provided information,
- f. the security breach and data loss incident reporting procedures,
- g. the basic understanding of procedures to protect the network from malware attacks,
- h. spoofing, phishing and pharming, and network fraud prevention, and
- i. the possible criminal and civil sanctions and penalties for misuse of SSA-provided information.

SSA requires the EIEP to provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful access and/or disclosure.

## Exhibit F, Attachment B

SSA requires the EIEP to provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, or agent who views SSA-provided information also certify that they understand the potential criminal and administrative sanctions or penalties for unlawful disclosure. SSA requires the state agency to require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. The non-disclosure attestation must also include acknowledgement from each employee, contractor, and agent that he or she understands and accepts the potential criminal and/or civil sanctions or penalties associated with misuse or unauthorized disclosure of SSA-provided information. The state agency must retain the non-disclosure attestations for at least five (5) to seven (7) years for each individual who processes, views, or encounters SSA-provided information as part of their duties.

SSA strongly recommends the use of login banners, emails, posters, signs, memoranda, special events, and other promotional materials to encourage security awareness throughout your enterprise.

The state agency must designate a department or party to take the responsibility to provide ongoing security awareness training for all employees, contractors, and agents who access SSA-provided information. Training must include:

- The sensitivity of SSA-provided information and address the Privacy Act and other Federal and state laws governing its use and misuse
- Rules of behavior concerning use and security in systems processing SSA-provided information
- Restrictions on viewing and/or copying SSA-provided information
- The employee, contractor, and agent's responsibility for proper use and protection of SSA-provided information
- Proper disposal of SSA-provided information
- Security incident reporting procedures
- Basic understanding of procedures to protect the network from malware attacks



## **Exhibit F, Attachment B**

- **Spoofing, Phishing and Pharming scam prevention**
- **The possible sanctions and penalties for misuse of SSA-provided information**

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

**5.11 Contractors of Electronic Information Exchange Partners**  
*(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Risk Assessment (RA), System and Services Acquisition (SA), Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)*

The state agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by the Agreement may be subject to both civil and criminal sanctions pursuant to applicable Federal statutes. The state agency will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing the Agreement, and thereafter at SSA's request, the state agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

Contractors of the state agency must adhere to the same security requirements as employees of the state agency. The state agency is responsible for the oversight of its contractors and the contractor's compliance with the security requirements. The state agency must enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties. Such contractors or agents agree to abide by all relevant Federal laws, restrictions on access, use, disclosure, and the security requirements contained within the state agency's agreement with SSA.

The state agency must provide proof of the contractual agreement with all contractors and agents who encounter SSA-provided information as part of their duties. If the contractor processes, handles, or transmits information provided to the state agency by SSA or has authority to perform on the state agency's behalf, the state agency should clearly state the specific roles and functions of the contractor within the agreement. The state agency will provide SSA written certification that the contractor is meeting the terms of the agreement, including SSA security requirements. The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to SSA-provided information.

The state agency must also require that contractors and agents who will process, handle, or transmit information provided to the state agency by SSA to include language in their signed agreement that obligates the contractor to follow the terms of the state agency's data exchange agreement with SSA. The state agency must also make certain that the contractor and agent's employees receive the same security awareness training as the state agency's employees. The state agency, the contractor, and the agent should maintain awareness-training records for their employees and require the same mandatory annual

## Exhibit F, Attachment B

certification procedures.

SSA requires the state agency to subject the contractor to ongoing security compliance reviews that must meet SSA standards. The state agency will conduct compliance reviews at least triennially commencing no later than three (3) years after the approved initial security certification to SSA. The state agencies will provide SSA with documentation of their recurring compliance reviews of their contractors and agents. The state agencies will provide the documentation to SSA during their scheduled compliance and certification reviews or upon SSA's request.

If the state agency's contractor will be involved with the processing, handling, or transmission of information provided to the EIEP by SSA offsite from the EIEP, the EIEP must have the contractual option to perform onsite reviews of that offsite facility to ensure that the following meet SSA's requirements:

- a) safeguards for sensitive information,
- b) technological safeguards on computer(s) that have access to SSA-provided information,
- c) security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and redisclosure of SSA-provided information, and
- d) continuous monitoring of the EIEP contractors or agent's network infrastructures and assets.

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

## 5.12 Cloud Service Providers (CSP) for Electronic Information Exchange Partners

*(NIST SP 800-144, NIST SP 800-145, NIST SP 800-146, OMB Memo M-14-03, NIST SP 137)*

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 defines Cloud Computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.” The three service models, as defined by NIST SP 800-145 are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The Deployment models are Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud. Furthermore, The Federal Risk and Authorization Program (FedRAMP) is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

SSA requires the State Agency, contractor(s), and agent(s) to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

SSA requires the State Agency, contractor(s), and agent(s) to agree that any state-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a “de facto” extension of the State Agency and is subject to onsite inspection and review by the State Agency or SSA with prior notice.

SSA requires that the State Agency thoroughly describe all specific contractual obligations of each party to the Cloud Service Provider (CSP) agreement between the state agency and the CSP vendor(s). If the obligations, services, or conditions widely differ from agency to agency, we require separate SDP Questionnaires to address the CSP services provided to each state agency involved in the receipt, processing, storage, or disposal of SSA-provided information.

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

## **6. Security Certification and Compliance Review Programs**

*(NIST SP 800-18 – System Security Plans and Planning (PL) Family, NIST SP 800-53 rev. 4)*

SSA's security certification and compliance review programs are distinct processes. The certification program is a unique episodic process when an EIEP initially requests electronic access to SSA-provided information or makes substantive changes to existing exchange protocol, delivery method, infrastructure, or platform. The certification process entails two stages (refer to 6.1 for details) intended to ensure that management, operational, and technical security measures work as designed. SSA must ensure that the EIEPs fully conform to SSA's security requirements at the time of certification and satisfy both stages of the certification process before SSA will permit online access to its data in a production environment.

The compliance review program entails cyclical security review of the EIEP performed by, or on behalf of SSA. The purpose of the review is to assess an EIEP's conformance to SSA's current security requirements at the time of the review engagement. The compliance review program applies to both online and batch access to SSA-provided information. Under the compliance review program, EIEPs are subject to ongoing and periodic security reviews by SSA.

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

**6.1 The Security Certification Program**  
*(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)*

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

- a) **Phase 1:** The Security Design Plan (SDP) is a formal written plan authored by the EIEP to document its management, operational, and technical security controls to safeguard SSA-provided information (refer to *Documenting Security Controls in the Security Design Plan*).

**NOTE:** SSA may have legacy EIEPs (EIEPs not certified under the current process) who have not prepared an SDP. SSA strongly recommends that these EIEPs prepare an SDP.

The EIEP's preparation and maintenance of a current SDP will aid them in determining potential compliance issues prior to reviews, assuring continued compliance with SSA's TSSRs, and providing for more efficient security reviews.

- b) **Phase 2:** The SSA Onsite Certification is a formal security review conducted by SSA, or on its behalf, to examine the full suite of management, operational, and technical security controls implemented by the EIEP to safeguard data obtained from SSA electronically (refer to *The Certification Process*).

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

## 6.2 Documenting Security Controls in the SDP

*(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)*

### 6.2.1 When an SDP is required:

**EIEPs must submit an SDP when one or more of the following circumstances apply:**

- a) to obtain approval for requested access to SSA-provided information for an initial agreement,
- b) to obtain approval to reestablish previously terminated access to SSA-provided information,
- c) to obtain approval to implement a new operating or security platform that will involve SSA-provided information,
- d) to obtain approval for significant changes to the EIEP's organizational structure, technical processes, operational environment, or security implementations planned or made since approval of their most recent SDP or of their most recent successfully completed security review,
- e) to confirm compliance when one or more security breaches or incidents involving SSA-provided information occurred since approval of the EIEP's most recent SDP or of their most recent successfully completed security review,
- f) to document descriptions and explanations of measures implemented as the result of a data breach or security incident,
- g) to document descriptions and explanations of measures implemented to resolve non-compliance issue(s), and
- h) to obtain a new approval after SSA revoked approval of the most recent SDP

**SSA may require a new SDP if changes occurred (other than those listed above) that may affect the terms of the EIEP's data exchange agreement with SSA.**

***SSA will not approve the SDP or allow the initiation of transactions and/or access to SSA-provided information before the EIEP complies with the TSSRs.***

**NOTE: EIEPs that function only as an STC, transferring SSA-provided information to other EIEPs must, per the terms of their agreements with SSA, adhere to SSA's TSSR and exercise their responsibilities regarding protection of SSA-provided information. (See Page 48 Definition of STC)**

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



### 6.3 The Certification Process

*(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)*

Once the EIEP has successfully satisfied Phase 1, SSA will conduct an onsite certification review. The objective of the onsite review is to ensure the EIEP's management, operational, and technical controls safeguarding SSA-provided information from misuse and improper disclosure and that those safeguards function and work as intended.

At its discretion, SSA may request the EIEP to participate in an onsite review and compliance certification of their security infrastructure.

The onsite review may address any or all of SSA's security requirements and include, when appropriate:

- 1) a demonstration of the EIEP's implementation of each security requirement,
- 2) a physical review of pertinent supporting documentation to verify the accuracy of responses in the SDP,
- 3) a demonstration of the functionality of the software interface for the system that will receive, process, and store SSA-provided information,
- 4) a demonstration of the Automated Audit Trail System (ATS),
- 5) a walkthrough of the EIEP's data center to observe and document physical security safeguards,
- 6) a demonstration of the EIEP's implementation of electronic exchange of data with SSA,
- 7) a discussions with managers, supervisors, information security officers, system administrators, or other state stakeholders,
- 8) an examination of management control procedures and reports pertaining to anomaly detection or anomaly prevention,
- 9) a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,

- 10) a demonstration of the permission module or similar design, to show how the system triggers requests for information from SSA,
- 11) a demonstration of how the process for requests for SSA-provided information prevents SSNs not present in the EIEP's system from sending requests to SSA.

**We may attempt to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEPs system.**

During a certification or compliance review, SSA or a certifier acting on its behalf, may request a demonstration of the EIEP's ATS and its record retrieval capability. SSA or a certifier may request a demonstration of the ATS' capability to track the activity of employees who have the potential to access SSA-provided information within the EIEP's system. The certifier may request more information from those EIEPs who use an STC to handle and audit transactions. SSA or a certifier may conduct a demonstration to see how the EIEP obtains audit information from the STC regarding the EIEP's SSA transactions.

If an STC handles and audits an EIEP's transactions, SSA requires the EIEP to demonstrate both their in-house audit capabilities and the process used to obtain audit information from the STC.

If the EIEP employs a contractor or agent who processes, handles, or transmits the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include the contractor's facility in the onsite certification review. The inspection may occur with or without a representative of the EIEP.

Upon successful completion of the onsite certification review, SSA will authorize electronic access to production data by the EIEP. SSA will provide written notification of its certification to the EIEP and all appropriate internal SSA components.

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

**6.5 The Compliance Review Program and Process**  
*(NIST SP 800-18 – System Security Plans, Configuration Management (CM), Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)*

Similar to the certification process, the compliance review program entails a process intended to ensure that EIEPs that receive electronic information from SSA are in full compliance with the SSA's TSSRs. SSA requires EIEPs to complete and submit (based on a timeline agreed upon by SSA and EIEP's stakeholders) a Compliance Review Questionnaire (CRQ). The CRQ (similar to the SDP), describes the EIEP's management, operational, and technical controls used to protect SSA-provided information from misuse and improper disclosure. We also want to verify that those safeguards function and work as intended.

As a practice, SSA attempts to conduct compliance reviews following a 3-5 year periodic review schedule. However, as circumstances warrant, a review may take place at any time. Three prominent examples that would trigger an ad hoc review are:

- A. a significant change in the outside EIEP's computing platform,
- B. a violation of any of SSA's TSSRs, or
- C. an unauthorized disclosure of SSA-provided information by the EIEP.

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

SSA may, at its discretion, request that the EIEP participate in an onsite compliance review of their security infrastructure to confirm the implementation of SSA's security requirements.

The onsite review may address any or all of SSA's security requirements and include, where appropriate:

- D. a demonstration of the EIEP's implementation of each requirement
- E. a random sampling of audit records and transactions submitted to SSA
- F. a walkthrough of the EIEP's data center to observe and document physical security safeguards
- G. a demonstration of the EIEP's implementation of online exchange of data with SSA,

## Exhibit F, Attachment B

- H. a discussion with managers, supervisors, information security officers, system administrators, or other state stakeholders,
  - I. an examination of management control procedures and reports pertaining to anomaly detection and prevention reports,
  - J. a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,
  - K. a demonstration of how a permission module or similar design triggers requests for information from SSA, and
  - L. a demonstration of how a permission module prevents the EIEP's system from processing SSNs not present in the EIEP's system.
- 1) We can accomplish this by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEP's system.**

SSA may perform an onsite or remote review for reasons including, but not limited, to the following:

- a) the EIEP has experienced a security breach or incident involving SSA-provided information
- b) the EIEP has unresolved non-compliance issue(s)
- c) to review an offsite contractor's facility that processes SSA-provided information
- d) the EIEP is a legacy organization that has not yet been through SSA's security certification and compliance review programs
- e) the EIEP requested that SSA perform an IV & V (Independent Verification and Validation review)

During the compliance review, SSA, or a certifier acting on its behalf, may request a demonstration of the system's audit trail and retrieval capability. The certifier may request a demonstration of the system's capability for tracking the activity of employees who view SSA-provided information within the EIEP's system. The certifier may request EIEPs that have STCs that handle and audit transactions with SSA to demonstrate the process used to obtain audit information from the STC.

If an STC handles and audits the EIEP's transactions with SSA, we may require the EIEP to demonstrate both their in-house audit capabilities and the processes used to

obtain audit information from the STC regarding the EIEP's transactions with SSA.

If the EIEP employs a contractor who will process, handle, or transmit the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include in the onsite compliance review an onsite inspection of the contractor's facility. The inspection may occur with or without a representative of the EIEP. The format of the review in routine circumstances (e.g., the compliance review is not being conducted to address a special circumstance, such as a disclosure violation, etc.) will generally consist of reviewing and updating the EIEP's compliance with the systems security requirements described above in this document. At the conclusion of the review, SSA will issue a formal report to appropriate EIEP personnel. The Compliance Report will address findings and recommendations from SSA's compliance review, which includes a plan for monitoring each issue until closure.

***NOTE: SSA will never request documentation for compliance reviews unless necessary to assess the EIEP's security posture. The information is only accessible to authorized individuals who have a need for the information as it relates to the EIEP's compliance with its electronic data exchange agreement with SSA and the associated system security requirements and procedures. SSA will not retain the EIEP's documentation any longer than required. SSA will delete, purge, or destroy the documentation when the retention requirement expires.***

Compliance Reviews are either on-site or remote reviews. High-risk reviews must be onsite reviews, medium risk reviews are usually onsite, and low risk reviews may qualify for a remote review via telephone. The past performance of the entire state determines whether a review is onsite or remote **SSA determines a state's risk level based on the "high water mark principle."** If one agency is high risk, the entire state is high risk. The following is a high-level example of the analysis that aids SSA in making a preliminary determination as to which review format is appropriate. SSA may also use additional factors to determine whether SSA will perform an onsite or remote compliance review.

#### **A. High/Medium Risk Criteria**

- 1) undocumented closing of prior review finding(s),
- 2) implementation of management, operational or technical controls that affect security of SSA-provided information (e.g. implementation of new data access method), or
- 3) a reported PII breach within the state.

**B. Low Risk Criteria**

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

**6.5.1 EIEP Compliance Review Participation**

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

- a) a sample of managers, supervisors, information security officers, system administrators, etc. responsible for enforcing and monitoring ongoing compliance to security requirements and procedures to assess their level of training to monitor their employee's use of SSA-provided information, and for reviewing reports and taking necessary action
- b) the individuals responsible for performing security awareness and employee sanction functions to learn how EIEPs fulfill this requirement
- c) a sample of the EIEP's employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA-provided information
- d) the individual(s) responsible for management oversight and quality assurance functions to confirm how the EIEP accomplishes this requirement
- e) any additional individuals as deemed appropriate by SSA (i.e. analysts, Project/Program Manager, claims reps, etc.)

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