SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

A0²

FROM: Executive Office

SUBMITTAL DATE:
February 25, 2014

SUBJECT: Approval of Agreement for Disclosure and Use of Medi-Cal Data (Data Use Agreement) for the Low Income Health Program known as Riverside County HealthCare. All Districts [$0]

RECOMMENDED MOTION: That the Board of Supervisors:
1. Approve and authorize Chairman of the Board to sign the Agreement for Disclosure and Use of Medi-Cal Data (Data Use Agreement) between the County of Riverside and the Department of Health Care Services (DHCS) to address the conditions under which DHCS will disclose and the County will obtain and use Medi-Cal data file(s).

BACKGROUND:
Summary
The Low Income Health Program (LIHP), in Riverside County known as Riverside County HealthCare (RCHC), was a two year program that was a component of the State's renewed Section 1115(a) Comprehensive Demonstration Project Waiver expanding health care coverage to low income, uninsured adults who were not eligible for Medi-Cal or other public programs. On February 9, 2011, Board of Supervisors agenda item 3:27; authorized submission of the LIHP application to DHCS. The County of

Debra Cournoyer
Deputy County Executive Officer

FORM APPROVED COUNTY COUNSEL
BY: NEAL R. KIPNIS
DATE 2/14/14
Departmental Concurrence

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost:	POLICY/CONSENT (per Exec. Office)
COST	$ 0.00	$ 0.00	$ 0.00	$ 0.00	Consent ☐ Policy ☐
NET COUNTY COST	$ 0.00	$ 0.00	$ 0.00	$ 0.00	

SOURCE OF FUNDS: N/A

Budget Adjustment: No

For Fiscal Year: 2013-14

C.E.O. RECOMMENDATION: APPROVE
BY:
George A. Johnson
County Executive Office Signature

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Jeffries, seconded by Supervisor Stone and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes: Jeffries, Tavaglione, Stone, Benoit and Ashley
Nays: None
Absent: None
Date: February 25, 2014
xc: E.O.

Kecia Harper-Ihem
Clerk of the Board
By:
Deputy

☐ Positions Added
☐ Change Order
A-30
4/5 Vote
☐
☐

Prev. Agn. Ref.: 6/28/2011, 3.15; 1/31/12, 3.2;   **District:** All   **Agenda Number:**

3-3

SUBMITTAL TO THE BOARD OF SUPERVISORS, COUNTY OF RIVERSIDE, STATE OF CALIFORNIA
FORM 11: Approval of Agreement for Disclosure and Use of Medi-Cal Data (Data Use Agreement) for the Low Income Health Program known as Riverside County HealthCare.

DATE: February 25, 2014
PAGE: Page 2 of 2

BACKGROUND:
Summary (continued)

Riverside received initial approval from DHCS on April 11, 2011. The approval by DHCS initiated the concurrent authorization and contract process, which continued until all program requirements were met and program terms were finalized. On June 28, 2011, Board of Supervisors agenda item 3.15; authorized the Assistant County Executive Officer to sign the contract between the DHCS and the County of Riverside. On January 31, 2012, Board of Supervisors agenda item 3.2; the Board ratified the contract between the County and the State DHCS for implementation of the LIHP.

This data use agreement addresses the conditions under which DHCS will disclose and the County will obtain and use Medi-Cal data file(s). This agreement is necessary to meet Health Insurance Portability and Accountability Act (HIPAA) requirements regarding accessing of confidential LIHP data after December 31, 2013. The LIHP data will be accessed for the purposes, including but not limited to, late enrollees (those enrollees determined eligible for the RCHC program after November 20, 2013), program evaluation update data, and file corrections, etc.

Impact on Citizens and Businesses

This agreement meets regulatory requirements to protect Riverside County HealthCare enrollee protected health information in accordance with HIPAA.

SUPPLEMENTAL:
Additional Fiscal Information

There is no cost associated with this agreement.

Contract History and Price Reasonableness

This is a requirement associated with previously executed agreements with the DHCS. Price reasonableness is not applicable to this data use agreement as there is no cost.

DEPARTMENT OF HEALTH CARE SERVICES

AGREEMENT FOR DISCLOSURE AND USE OF MEDI-CAL DATA

In order to secure data and documents that reside in the California Department of Health Care Services (DHCS) Medi-Cal systems of records, or with its agents, and to ensure the integrity, security, and confidentiality of such data and documents, and to permit only appropriate disclosure and use as may be permitted by law, DHCS and Riverside County (parties) enter into this Agreement to comply with the following specific sections. This Agreement shall be binding on any successors to the parties.

1. This Agreement is by and between the DHCS and Riverside County User(s).

2. This Agreement addresses the conditions under which DHCS will disclose and the User(s) will obtain and use Medi-Cal data file(s).This Agreement supplements any agreements between the parties with respect to the use of information from data and documents and overrides any contrary instructions, directions, agreements, or other understandings in or pertaining to any other prior communication from DHCS or any of its components with respect to the data specified in this Agreement. The terms of this Agreement may be changed only by a written modification to this Agreement or by the parties entering into a new agreement. The parties agree further that instructions or interpretations issued to the User(s) concerning this Agreement, and the data and documents specified herein, shall not be valid unless issued in writing by the DHCS point-of-contact specified in Section 4 or the DHCS signatories to this Agreement shown in Section 22.

3. The parties mutually agree that the following named individuals are designated as "Custodians of the Files" on behalf of the User(s) and shall be responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use or disclosure. The User(s) agree to notify DHCS within fifteen (15) days of any change to the custodianship information.

Supervisor Jeff Stone
(Name of Custodian of Files)

Chairman
(Title/Component)

Board of Supervisors
(Company/Organization)

4080 Lemon Street, Riverside, CA 92501
(Company Address)

(951) 955-1000
(Phone Number / Email Address)

1

4. The parties mutually agree that the following named individual will be designated as "point-of-contact" for the Agreement on behalf of DHCS.

Kimberly Swift
(Name of Contact)

Associate Governmental Program Analyst
Low Income Health Program Division
Low Income Health Program Implementation Section
Program Policy Unit
(Title/Component)

(916) 322-5179, Kimberly.Swift@dhcs.ca.gov
(Phone Number / Email Address)

5. The parties mutually agree that the following specified Attachments are part of this Agreement:

Attachment A: Business Associate Addendum
Attachment B: Social Security Administration Agreement

6. The parties mutually agree, and in furnishing data files hereunder DHCS relies upon such agreement, that such data file(s) will be used solely for the following purposes:

The Business Associate Agreement attached to contract No. 11-15909-RI-13 between DHCS and Riverside County will be extended for a year from the date this DUA is signed by the parties. The extension of the BAA allows the health department LIHP eligibility workers to make timely adjustments to Medi-Cal Eligibility Data Systems (MEDS) records to mitigate any issues that may arise in eligibility reporting which affect continuous Medi-Cal managed care plan coverage for the transition population.

7. Some of the data specified in this Agreement may constitute Protected Health Information (PHI), including protected health information in electronic media (ePHI), under federal law, and personal information (PI) under state law. The parties mutually agree that the creation, receipt, maintenance, transmittal and disclosure of data from DHCS containing PHI or PI shall be subject to the provisions of 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 (HITECH Act) and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 (HIPAA regulations), the provisions of the California Information Practices Act, Civil Code section 1798 et. seq., 42 CFR Part 2, and the provisions of other applicable federal and state law. User(s) specifically agree they will not use the data for any purpose other than that stated in paragraph 6 of this Agreement. User(s) also specifically agree they will not use any DHCS data, by itself or in combination with any other data from any source, whether publicly available or not, to individually identify any person except for the purposes set forth in section 6, and will not disclose the DHCS data to anyone other than DHCS as provided in this Agreement and in 42 CFR Section 2.53(d).

8. The following definitions shall apply to this Agreement. The terms used in the attached BAA but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations or other applicable law. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

2

a. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations and the California Information Practices Act.

b. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.

c. Personal Information (PI) shall have the meaning given to such term in Civil Code section 1798.29.

d. Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.

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

f. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.

g. Unsecured PHI shall have the meaning given to such term under the HITECH Act, any guidance issued pursuant to such Act including, but not limited to, 42 USC section 17932(h), and the HIPAA regulations.

9. The User(s) represent and warrant that the User(s) shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement to any person, company or organization except for the purposes set forth in section 6 in this Agreement or as DHCS shall authorize in writing. The User(s) agrees that, within the User(s)' organizations, access to the data covered by this Agreement shall be limited to the minimum number of individuals necessary to achieve the purposes set forth in section 6 in this Agreement and Attachment A and to those individuals on a need-to-know basis only. User(s) shall not use or further disclose the information other than is permitted by this Agreement or as otherwise required by law. The User(s) shall not use the information to identify or contact any individuals except for the purposes set forth in section 6 in this Agreement.

3

User Initial: _____

10. The User(s) agree to notify DHCS within 30 days of the completion of the purpose specified in section 6. Upon such completion, the User(s) shall destroy all electronic data files provided by DHCS pursuant to this Agreement by wiping such data using Department of Defense standards or as approved by DHCS. The Users will also no longer have access to MEDS. The User(s) shall destroy all paper documents with the data provided by DHCS, except for the purposes set forth in section 6 in this Agreement, by using a confidential method of destruction, such as crosscut shredding or contracting with a company that specializes in confidential destruction of documents. The User(s) shall certify the destruction of the file(s) in writing within 30 days of the destruction. A statement certifying this action must be sent to the DHCS point-of-contact listed in section 4. The User(s) agree that no data from DHCS records, any parts or copies thereof, including files derived from DHCS records (electronic, hardcopy or otherwise), shall be retained when the files are destroyed, except for the purposes set forth in section 6 in this Agreement, unless authorization in writing for the retention of such files has been received from the DHCS person designated in section 4.

11. The User(s) agree to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established in HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH), in 45 CFR, parts 160, 162 and 164 of the HIPAA Privacy and Security Regulations. The User(s) also agree to provide 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. If the data obtained by User(s) from DHCS includes data provided to DHCS by the Social Security Administration (SSA), 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 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. In addition, the User(s) agree to comply with the specific security controls enumerated in Attachment A of this Agreement. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide DHCS data, agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information.

12. The User(s) acknowledge that in addition to the requirements of this Agreement, they must also abide by the privacy and disclosure laws and regulations under 45 CFR Parts 160, 162 and 164, of the HIPAA regulations, section 14100.2 of the California Welfare & Institutions Code, Civil Code section 1798.1 et seq., and Confidentiality of Alcohol and Drug Abuse Patient (ADP) Records law, 42 CFR Part 2, as well as any other applicable state or federal law or regulation. 42 CFR section 2.1(b)(2)(B) and section 2.53(c) allow for the disclosure of ADP records for the purpose of Medicaid audit or evaluation. User(s) acknowledge that 42 CFR Section 2.53(d) limits the use and re-disclosure of the information provided by DHCS: (d) Limitations on disclosure and use. Except as provided in paragraph (c) of this section, patient identifying information disclosed under this section may be disclosed only back to the program

4

from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by a court order entered under § 2.66 of these regulations.

The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide the DHCS data, as agreed upon by DHCS, agree to the same restrictions and conditions that apply to the User(s) with respect to such information.

13. The User(s) agree to report to DHCS any use or disclosure of the information not provided for by this Agreement of which it becomes aware, immediately upon discovery, and to take further action regarding the use or disclosure as specified in Attachment C, Notification of Breach, of this Agreement.

14. User(s) agree to train, and use reasonable measures to ensure compliance with the requirements of this Agreement by, employees who assist in the performance of functions or activities under this Agreement and use or disclose DHCS data, and to discipline such employees who intentionally violate any provisions of this Agreement, including by termination of employment. In complying with the provisions of this section, User(s) shall observe the following requirements:

(a) User(s) shall provide information privacy and security training, at least annually, at its own expense, to all its employees who assist in the performance of functions or activities under this Agreement and use or disclose DHCS data; and

(b) User(s) shall require each employee who receives information privacy and security training to sign a certification, indicating the employee's name and the date on which the training was completed.

15. From time to time, DHCS may, upon prior written notice and at mutually convenient times, inspect the facilities, systems, books and records of User(s) to monitor compliance with this Agreement. User(s) shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the DHCS Privacy Officer in writing. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, User(s)' facilities, systems and procedures does not relieve User(s) of their responsibility to comply with this Agreement.

16. The User(s) acknowledge that penalties under 45 CFR, parts 160, 162 and 164 of the HIPAA regulations, and section 14100.2 of the California Welfare & Institutions Code, including possible fines and imprisonment, may apply with respect to any disclosure of information in the file(s) that is inconsistent with the terms of this Agreement. The User(s) further acknowledge that criminal penalties under the Confidentiality of Medical Information Act (Civ. Code § 56) may apply if it is determined that the User(s), or any individual employed or affiliated therewith, knowingly and willfully obtained any data under false pretenses.

17. By signing this Agreement, the User(s) agree to abide by all provisions set out in this Agreement and in Attachments A and B and for protection of the data file(s) specified in this Agreement, and acknowledge having received notice of potential criminal, administrative, or civil penalties for violation of the terms of the Agreement. The User(s) agree that any material violations of the terms of this Agreement or any of the laws and regulations governing the use of DHCS data may result in denial of access to DHCS data. Further, the User(s) agree to abide by the terms to the Business Associate Agreement attached hereto and incorporated herein as Attachment C.

5

18. This Agreement shall terminate at the time of the completion of the purposes set forth in section 6 in this Agreement or one year after the date it is executed, whichever event occurs sooner, and at that time all data provided by DHCS must be destroyed as set forth in section 10, above, and a certificate of destruction sent to the DHCS representative named in section 4, unless data has been destroyed prior to the termination date and a certificate of destruction sent to DHCS. All representations, warranties and certifications shall survive termination.

Termination for Cause. Upon DHCS' knowledge of a material breach or violation of this Agreement by User(s), DHCS may provide an opportunity for User(s) to cure the breach or end the violation and may terminate this Agreement if User(s) does not cure the breach or end the violation within the time specified by DHCS. DHCS may terminate this Agreement immediately if User(s) has breached a material term and DHCS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, User must destroy all PHI and PI in accordance with Section 10, above. The provisions of this Agreement governing the privacy and security of the PHI and PCI shall remain in effect until all PHI and PI is destroyed or returned to DHCS.

19. This Agreement may be signed in counterpart and all parts taken together shall constitute one agreement.

20. The Custodian, as named in Section 3, hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the User(s), and agrees in a representative capacity to comply with all of the provisions of this Agreement on behalf of the User(s).

_Supervisor Jeff Stone_____
(Name of Custodian of File(s) - Typed or Printed)

_Chairman_____
(Title/Component)

FEB 2 5 2014

(Signature)   (Date)

ATTEST:
KECIA HARPER-IHEM, Clerk

By _____
        DEPUTY

FORM APPROVED COUNTY COUNSEL
BY: _____
    NEAL R. KIPNIS   DATE

6

User Initial: _____

DUA No. 2013-DHCSLIHP-009
LIHP Contract No. 11-15909-RI-13

FEB 2 5 2014   3-3

21. On behalf of the User(s), the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Supervisor Jeff Stone
(Name - Typed or Printed)

Chairman
(Title/Component)

Board of Supervisors
(Company/Organization)

4080 Lemon Street
(Address)

Riverside, CA   92501
(City/State/ZIP Code)

(951) 955-1000
(Phone Number and E-Mail Address)

(Signature)   FEB 2 5 2014
(Date)

ATTEST:
KECIA HARPER-IHEM Clerk
By _____ DEPUTY

FORM APPROVED COUNTY COUNSEL
BY: NEAL R. KIPNIS
DATE

22. On behalf of DHCS, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Jalynne Callori   Bob BAXTER for
(Name of DHCS Representative - Typed or Printed)

Chief, Low Income Health Program Division
(Title/Component)

(Signature)   4/2/14
(Date)

7

User Initial: _____

DEPARTMENT OF HEALTH CARE SERVICES

AGREEMENT FOR DISCLOSURE AND USE OF MEDI-CAL DATA

Attachment A
HIPAA Business Associate Addendum

I. Recitals

A. This Contract (Agreement) has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ('the HITECH Act"), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").

B. The Department of Health Care Services ("DHCS") wishes to disclose to Business Associate 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, and personal information ("PI") under state law.

C. As set forth in this Agreement, Contractor, here and after, is the Business Associate of DHCS acting on DHCS' behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of DHCS and creates, receives, maintains, transmits, uses or discloses PHI and PI. DHCS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties."

D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI 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 DHCS must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act.

E. The terms used in this Addendum, 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.

II. 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. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.

DHCS HIPAA BAA 3/11

E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.

F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.

G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CRF Parts 160 and 164.

H. Personal Information shall have the meaning given to such term in California Civil Code section 1798.29.

I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.

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

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

L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.

M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.

N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act and the HIPAA regulations.

III. Terms of Agreement

A. Permitted Uses and Disclosures of PHI by Business Associate

Permitted Uses and Disclosures. Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of DHCS, provided that such use or disclosure would not violate the HIPAA regulations, if done by DHCS. Any such use or disclosure must,

2

to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

1. **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Addendum, Business Associate may:

    a. **Use and disclose for management and administration.** Use and disclose PHI for the proper management and administration of the Business Associate provided that such disclosures are required by law, or the Business Associate 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 Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

    b. **Provision of Data Aggregation Services.** Use PHI to provide data aggregation services to DHCS. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of DHCS 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 DHCS.

B. Prohibited Uses and Disclosures

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).

2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of DHCS and as permitted by 42 U.S.C. section 17935(d)(2).

C. Responsibilities of Business Associate

Business Associate agrees:

1. **Nondisclosure.** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by this Agreement or as required by law.

2. **Safeguards.** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of DHCS, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate 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 Business Associate's operations and the nature and scope of its activities, and which

incorporates the requirements of section 3, Security, below. Business Associate will provide DHCS with its current and updated policies.

3. **Security.** To 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, the Business Associate Data Security Requirements;

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

   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; and

   d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security 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, Business Associate must comply with changes to these standards that occur after the effective date of this Agreement.

   Business Associate 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 DHCS.

D. **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

E. **Business Associate's Agents and Subcontractors.**

1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of DHCS, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply 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 and PI. Business Associate shall incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PI be reported to Business Associate.

2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:

a. 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 DHCS; or

b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

F. **Availability of Information to DHCS and Individuals.** To provide access and information:

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

2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable DHCS to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).

3. If Business Associate receives data from DHCS that was provided to DHCS by the Social Security Administration, upon request by DHCS, Business Associate shall provide DHCS with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

G. **Amendment of PHI.** To make any amendment(s) to PHI that DHCS directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner designated by DHCS.

H. **Internal Practices.** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from DHCS, or created or received by Business Associate on behalf of DHCS, available to DHCS or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by DHCS or by the Secretary, for purposes of determining DHCS' 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 Business Associate, Business Associate shall so certify to DHCS and shall set forth the efforts it made to obtain the information.

I. **Documentation of Disclosures.** To document and make available to DHCS or (at the direction of DHCS) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for DHCS as of January 1, 2009, Business Associate 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 Business Associate acquires electronic health records for DHCS after

5

January 1, 2009, Business Associate 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.

J. **Breaches and Security Incidents.** During the term of this Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

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

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

   Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

   a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

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

2. **Investigation and Investigation Report.** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. Within 72 hours of the discovery, Business Associate shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer:

3. **Complete Report.** To provide a complete report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or

6

disclosure. The report shall be submitted on the "DHCS 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, the HIPAA regulations and/or state law. 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 DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide DHCS with such information. 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 "DHCS Privacy Incident Report" form. DHCS will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.

4. **Notification of Individuals.** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

5. **Responsibility for Reporting of Breaches.** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach immediately upon discovery of the breach. If Business Associate 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 DHCS in addition to Business Associate, Business Associate shall notify DHCS, and DHCS and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.

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

DHCS Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Fax: (916) 440-5537 Telephone: ITSD Service Desk (916) 440-7000 or (800) 579-0874

K. **Termination of Agreement.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by DHCS of this Addendum, it shall take the following steps:

1. Provide an opportunity for DHCS to cure the breach or end the violation and terminate the Agreement if DHCS does not cure the breach or end the violation within the time specified by Business Associate; or

2. Immediately terminate the Agreement if DHCS has breached a material term of the Addendum and cure is not possible.

L. **Due Diligence.** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum 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 Addendum.

M. **Sanctions and/or Penalties.** Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

IV. Obligations of DHCS

DHCS agrees to:

A. **Notice of Privacy Practices.** Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR section 164.520, as well as any changes to such notice. Visit the DHCS Privacy Office to view the most current Notice of Privacy Practices at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx or the DHCS website at www.dhcs.ca.gov (select "Privacy in the left column and "Notice of Privacy Practices" on the right side of the page).

8

B. ***Permission by Individuals for Use and Disclosure of PHI.*** Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.

C. ***Notification of Restrictions.*** Notify the Business Associate of any restriction to the use or disclosure of PHI that DHCS has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

D. ***Requests Conflicting with HIPAA Rules.*** Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations if done by DHCS.

V. Audits, Inspection and Enforcement

A. From time to time, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the DHCS Privacy Officer in writing. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does DHCS':

1. Failure to detect or

2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of DHCS' enforcement rights under this Agreement and this Addendum.

B. If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify DHCS and provide DHCS with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

VI. Termination

A. ***Term.*** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the contract and shall terminate when all the PHI provided by DHCS to Business Associate, or created or received by Business Associate on behalf of DHCS, is destroyed or returned to DHCS, in accordance with 45 CFR 164.504(e)(2)(ii)(I).

B. ***Termination for Cause.*** In accordance with 45 CFR section 164.504(e)(1)(ii), upon DHCS' knowledge of a material breach or violation of this Addendum by Business Associate, DHCS shall:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by DHCS; or

9

2. Immediately terminate this Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.

C. **Judicial or Administrative Proceedings.** Business Associate will notify DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. DHCS may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. DHCS may terminate this Agreement if a finding or stipulation that the Business Associate 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 Business Associate is a party or has been joined.

D. **Effect of Termination.** Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from DHCS (or created or received by Business Associate on behalf of DHCS) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify DHCS of the conditions that make the return or destruction infeasible, and DHCS and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

VII. Miscellaneous Provisions

A. **Disclaimer.** DHCS makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

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

1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by DHCS pursuant to this Section; or

2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that DHCS in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

C. **Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, available to DHCS at no cost to DHCS to

10

testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.

D. **No Third-Party Beneficiaries.** Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than DHCS or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

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

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

G. **Survival.** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of this Agreement.

H. **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

Attachment A
Business Associate Data Security Requirements

I. Personnel Controls

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

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

C. Confidentiality Statement. All persons that will be working with DHCS 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 DHCS PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.

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

II. Technical Security Controls

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

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

C. Minimum Necessary. Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

D. Removable media devices. All electronic files that contain DHCS 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 DHCS 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 DHCS 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.

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

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

H. **Data Destruction.** When no longer needed, all DHCS 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 DHCS Information Security Office.

I. **System Timeout.** The system providing access to DHCS 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 DHCS 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 DHCS PHI or PI, or which alters DHCS 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 DHCS 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 DHCS 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 DHCS 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 PHI can be encrypted. This requirement pertains to any type of 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 DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

III. Audit Controls

A. *System Security Review.* All systems processing and/or storing DHCS 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 DHCS 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 DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

IV. Business Continuity / Disaster Recovery Controls

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

B. *Data Backup Plan.* Contractor must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS 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 DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

V. Paper Document Controls

A. *Supervision of Data.* DHCS 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. DHCS 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 DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

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

D. *Removal of Data.* DHCS PHI or PI must not be removed from the premises of the Contractor except with express written permission of DHCS.

E. *Faxing.* Faxes containing DHCS 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 of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI in a single package shall be sent using a tracked mailing

14

method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.

DEPARTMENT OF HEALTH CARE SERVICES

AGREEMENT FOR DISCLOSURE AND USE OF MEDI-CAL DATA

Attachment B

Information Exchange Agreement between the Social Security Administration (SSA)
And The California Department of Health Care Services (State Agency)

1

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

A. **PURPOSE:** The purpose of this Information Exchange Agreement ("IEA") is to establish terms, conditions, and safeguards under which SSA will disclose to the State Agency certain information, records, or data (herein "data") to assist the State Agency in administering certain federally funded state-administered benefit programs (including state-funded state supplementary payment programs under Title XVI of the Social Security Act) identified in this IEA. By entering into this IEA, the State Agency agrees to comply with:

- the terms and conditions set forth in the Computer Matching and Privacy Protection Act Agreement ("CMPPA Agreement") attached as **Attachment 1**, governing the State Agency's use of the data disclosed from SSA's Privacy Act System of Records; and
- all other terms and conditions set forth in this IEA.

B. **PROGRAMS AND DATA EXCHANGE SYSTEMS:** (1) The State Agency will use the data received or accessed from SSA under this IEA for the purpose of administering the federally funded, state-administered programs identified in **Table 1** below. In **Table 1**, the State Agency has identified: (a) each federally funded, state-administered program that it administers; and (b) each SSA data exchange system to which the State Agency needs access in order to administer the identified program. The list of SSA's data exchange systems is attached as **Attachment 2**:

TABLE 1

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

1

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

(2) The State Agency will use each identified data exchange system _only_ for the purpose of administering the specific program for which access to the data exchange system is provided. SSA data exchange systems are protected by the Privacy Act and federal law prohibits the use of SSA's data for any purpose other than the purpose of administering the specific program for which such data is disclosed. In particular, the State Agency will use: (a) the **tax return data** disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to Section 1137 programs and child support enforcement programs in accordance with 26 U.S.C. § 6103(1)(8); and (b) the **citizenship status data** disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3, only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants. The State Agency also acknowledges that SSA's citizenship data may be less than 50 percent current. Applicants for SSNs report their citizenship data at the time they apply for their SSNs; there is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files a claim for benefits.

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

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

TABLE 2

TRANSFER OF DATA
☐ Data will be transmitted directly between SSA and the State Agency.
[X] Data will be transmitted directly between SSA and the California Office of Technology (State Transmission/Transfer Component ("STC")) by the File Transfer Management System, a secure mechanism approved by SSA. The STC will serve as the conduit between SSA and the State Agency pursuant to the State STC Agreement.
☐ Data will be transmitted directly between SSA and the Interstate Connection Network ("ICON"). ICON is a wide area telecommunications network connecting state agencies that administer the state unemployment insurance laws. When receiving data through ICON, the State Agency will comply with the "Systems Security Requirements for SSA Web Access to SSA Information Through the ICON," attached as **Attachment 3**.

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

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

G. SAFEGUARDING AND REPORTING RESPONSIBILITIES FOR PERSONALLY IDENTIFIABLE INFORMATION ("PII"):

1. The State Agency will ensure that its employees, contractors, and agents:
   a. properly safeguard PII furnished by SSA under this IEA from loss, theft or inadvertent disclosure;
   b. understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee, contractor, or agent is at his or her regular duty station;
   c. ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected;
   d. send emails containing PII only if encrypted or if to and from addresses that are secure; and
   e. limit disclosure of the information and details relating to a PII loss only to those with a need to know.

2. If an employee of the State Agency or an employee of the State Agency's contractor or agent becomes aware of suspected or actual loss of PII, he or she must immediately contact the State Agency official responsible for Systems Security designated below or his or her delegate. That State Agency official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact identified below. If, for any reason, the responsible State Agency official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the responsible State Agency official or delegate must call SSA's Network Customer Service Center ("NCSC") at 410-965-7777 or toll free at 1-888-772-6661 to report the actual or suspected loss. The responsible State Agency official or delegate will use the worksheet, attached as **Attachment 5**, to quickly gather and organize information about the incident. The responsible State Agency official or delegate must provide to SSA timely updates as any additional information about the loss of PII becomes available.

3. SSA will make the necessary contact within SSA to file a formal report in accordance with SSA procedures. SSA will notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of PII related to a data exchange under this IEA occurs.

4. If the State Agency experiences a loss or breach of data, it will determine whether or not to provide notice to individuals whose data has been lost of breached and bear any costs associated with the notice or any mitigation.

H. POINTS OF CONTACT:

FOR SSA

San Francisco Regional Office:

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

Data Exchange Issues:

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

Systems Issues:

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

Systems Security Issues:

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

FOR STATE AGENCY

Agreement Issues:

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

Technical Issues:

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

I. **DURATION:** The effective date of this IEA is January 1, 2010. This IEA will remain in effect for as long as: (1) a CMPPA Agreement governing this IEA is in effect between SSA and the State or the State Agency; and (2) the State Agency submits a certification in accordance with Section J. below at least 30 days before the expiration and renewal of such CMPPA Agreement.

J. **CERTIFICATION AND PROGRAM CHANGES**: At least 30 days before the expiration and renewal of the State CMPPA Agreement governing this IEA, the State Agency will certify in writing to SSA that: (1) it is in compliance with the terms and conditions of this IEA; (2) the data exchange processes under this IEA have been and will be conducted without change; and (3) it will, upon SSA's request, provide audit reports or other documents that demonstrate review and oversight activities. If there are substantive changes in any of the programs or data exchange processes listed in this IEA, the parties will modify the IEA in accordance with Section K. below and the State Agency will submit for SSA's approval new program questionnaires under Section C. above describing such changes prior to using SSA's data to administer such new or changed program.

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

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

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

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

ATTACHMENTS
1 — CMPPA Agreement
2 — SSA Data Exchange Systems
3 — Systems Security Requirements for SSA Web Access to SSA Information Through ICON
4 — Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration
5 — PII Loss Reporting Worksheet

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

SOCIAL SECURITY ADMINISTRATION

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

_5/13/05_
_____
Date

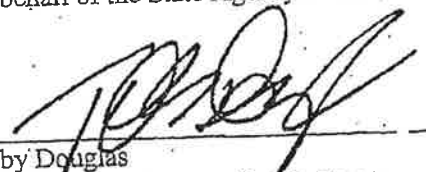## O. REGIONAL AND STATE AGENCY SIGNATURES:

SOCIAL SECURITY ADMINISTRATION
REGION IX

(signature)

Peter D. Spencer
San Francisco Regional Commissioner

10/26/09
Date

THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

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

(signature)

Toby Douglas
Chief Deputy Director, Health Care Programs

10/11/09
Date

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

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

1. The State Agency is in compliance with the terms and conditions of the IEA/F;

2. The State Agency has conducted the data exchange processes under the IEA/F without change, except as modified in accordance with the IEA/F;

3. The State Agency will continue to conduct the data exchange processes under the IEA/F without change, except as may be modified in accordance with the IEA/F;

4. Upon SSA's request, the State Agency will provide audit reports or other documents that demonstrate compliance with the review and oversight activities required under the IEA/F and the governing Computer Matching and Privacy Protection Act Agreement; and

5. In compliance with the requirements of the "Electronic Information Exchange Security Requirements, Guidelines, and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," 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

The State Agency will submit an updated Security Design Plan at least 30 days prior to making any changes to the areas listed above.

1

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

DEPARTMENT OF HEALTH CARE SERVICES OF CALIFORNIA

_____
Toby Douglas
Director

4/12/12
_____
Date

ATTACHMENT 1

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGRREMENT

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

I.   Purpose and Legal Authority

A.   Purpose.

This Computer Matching and Privacy Protection Act (CMPPA) Agreement between the Social Security Administration (SSA) and the California Health and Human Services Agency (State Agency), sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein "data") made by SSA to the State Agency that administers federally funded benefit programs under various provisions of the Social Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), including 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 Computer Matching and Privacy Protection Act 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 for state benefits from SSA Privacy Act Systems of Records (SOR) and verifies the Social Security numbers (SSN) of the applicants.

B.   Legal Authority

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

- Sections 1137, 453, and 1106(b) of the Act (42 U.S.C. §§ 1320b-7, 653, and 1306(b)) (income and eligibility verification data);
- 26 U.S.C. § 6103(l)(7) and (8) (tax return data);
- Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 401(x)(3)(B)(iv)) (prisoner data);
- Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii) (SSI);

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

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

II. Scope

A. The State Agency will comply with the terms and conditions of this Agreement and the Privacy Act, as amended by the CMPPA.

B. The State Agency will execute one or more Information Exchange Agreements (IEA) with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by the State Agency, the data elements that will be disclosed, and the data protection requirements implemented to assist the State Agency in the administration of those programs.

C. The State Agency will use the SSA data governed by this Agreement to determine entitlement and eligibility of individuals for one or more of the following programs:

1. Temporary Assistance to Needy Families (TANF) program under Part A of title IV of the Act;
2. Medicaid provided under an approved State plan or an approved waiver under title XIX of the Act;
3. State Children's Health Insurance Program (CHIP) under title XXI of the Act, as amended by the Children's Health Insurance Program Reauthorization Act of 2009;
4. Supplemental Nutritional Assistance Program (SNAP) under the Food Stamp Act of 1977 (7 U.S.C. § 2011, et seq.);

5. Women, Infants and Children Program (WIC) under the Child Nutrition Act of 1966 (42 U.S.C. § 1771, et seq.);
6. Medicare Savings Programs (MSP) under 42 U.S.C. § 1396a(10)(E);
7. Unemployment Compensation programs provided under a state law described in section 3304 of the Internal Revenue Code of 1954;
8. Low Income Heating and Energy Assistance (LIHEAP or home energy grants) program under 42 U.S.C. § 8621;
9. State-administered supplementary payments of the type described in section 1616(a) of the Act;
10. Programs under a plan approved under titles I, X, XIV or XVI of the Act;
11. Foster Care and Adoption Assistance under title IV of the Act;
12. Child Support Enforcement programs under section 453 of the Act (42 U.S.C. § 653);
13. Other applicable federally funded programs administered by the State Agency under titles I, IV, X, XIV, XVI, XVIII, XIX, XX and XXI of the Act; and
14. Any other federally funded programs administered by the State Agency that are compatible with SSA's programs.

D. The State Agency will ensure that SSA data disclosed for the specific purpose of administering a particular federally funded benefit program is used only to administer that program.

III. Justification and Expected Results

A. Justification

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

B. Expected Results

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

IV. Record Description

A. Systems of Records

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

- 60-0058 -- Master Files of SSN Holders and SSN Applications (accessible through EVS, SVES, or Quarters of Coverage Query data systems);
- 60-0059 -- Earnings Recording and Self-Employment Income System (accessible through BENDEX, SVES, or Quarters of Coverage Query data systems);
- 60-0090 -- Master Beneficiary Record (accessible through BENDEX or SVES data systems);
- 60-0103 -- Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB) (accessible through SDX or SVES data systems);
- 60-0269 -- Prisoner Update Processing System (PUPS) (accessible through SVES or Prisoner Query data systems).
- 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/gix/

C. Number of Records Involved

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

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

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

V. Notice and Opportunity to Contest Procedures

A. Notice to Applicants

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

B. Notice to Beneficiaries/Recipients/Annuitants

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

C. Opportunity to Contest

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

1. Inform the individual of the match findings and the opportunity to contest these findings;

2. Give the individual until the expiration of any time period established for the relevant program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond; and

3. Clearly state that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the SSA data are correct and will effectuate the threatened action or otherwise make the necessary adjustment to the individual's benefit or entitlement.

VI. Records Accuracy Assessment and Verification Procedures

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 they are 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.

SSA's citizenship data may be less than 50 percent current. Applicants 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 a claim for benefits.

VII. Disposition and Records Retention of Matched Items

A. The State Agency will retain all data received from SSA to administer programs governed by this Agreement only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.

B. The State Agency may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing the State Agency's retention of records.

C. The State Agency may use any accretions, deletions, or changes to the SSA data governed by this Agreement to update their master files of federally funded, state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing the State Agency's retention of records.

D. The State Agency may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this Agreement.

E. SSA will delete electronic data input files received from the State Agency after it processes the applicable match. SSA will retire its data in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

VIII. Security Procedures

The State Agency will comply with the security and safeguarding requirements of the Privacy Act, as amended by the CMPPA, related OMB guidelines; FISMA, related

NIST guidelines, and the current revision of IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities*, available at http://www.irs.gov. In addition, the State Agency will have in place administrative, technical, and physical safeguards for the matched data and results of such matches. Additional administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency, including specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

IX. Records Usage, Duplication, and Redisclosure Restrictions

A. The State Agency will use and access SSA data and the records created using that data only for the purpose of verifying eligibility for the specific federally funded benefit programs identified in the IEA.

B. The State Agency will comply with the following limitations on use, duplication, and redisclosure of SSA data:

1. The State Agency will not use or redisclose the data disclosed by SSA for any purpose other than to determine eligibility for, or the amount of, benefits under the state-administered income/health maintenance programs identified in this Agreement.

2. The State Agency will not use the data disclosed by SSA to 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.

3. 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 IRS Publication 1075.

4. The State Agency will use the citizenship status data disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3, only for the purpose of determining entitlement to Medicaid and CHIP programs for new applicants.

5. 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.

6. 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.

7. 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.

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.

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, 2012 (Effective Date) through December 31, 2013 (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 the OMB at least 40 days prior to the Effective Date.

3. Within 3 months prior the Expiration Date, the SSA DIB may, without additional review, renew this Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:

- the applicable data exchange will continue without any change; and
- SSA and the State Agency certify to the DIB in writing that the applicable data exchange has been conducted in compliance with this Agreement.

4. If either SSA or the State Agency does not wish to renew this Agreement, it must notify the other party of its intent not to renew at least 3 months prior to the Expiration Date.

B. Modification

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

C. Termination

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

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

XII. Reimbursement

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

XIII. Disclaimer

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

XIV. Points of Contact

A. SSA Point of Contact

Regional Office
Martin White, Director
San Francisco Regional Office, Center for Programs Support
1221 Nevin Ave
Richmond CA 94801
Phone: (510) 970-8243/Fax: (510) 970-8101
Martin.White@ssa.gov

B. State Agency Point of Contact

Sonia Herrera
Health and Human Services Agency
1600 Ninth Street, Room 460
Sacramento, CA 95814
Phone: (916) 654-3459/Fax: (916) 44-5001
sherrera@chhs.ca.gov

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

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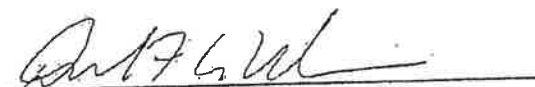
SOCIAL SECURITY ADMINISTRATION

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

1-17-2012
Date

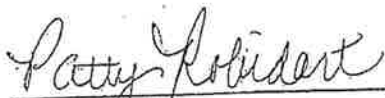I certify that the SSA Data Integrity Board approved the model of this CMPPA Agreement.

Daniel F. Callahan
Chair
SSA Data Integrity Board

1-26-2012
Date

XVI. Authorized Signatures

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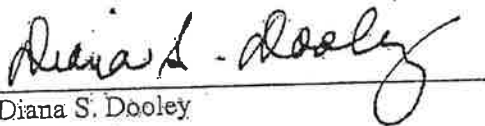
SOCIAL SECURITY ADMINISTRATION

Patty Robidert

fmz
Bill Zielinski
Regional Commissioner
San Francisco

05/10/2012
Date

HEALTH AND HUMAN SERVICES AGENCY

Diana S. Dooley

Diana S. Dooley
Secretary

April 27, 2012
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.

SVES (State Verification and Exchange System): A batch system that provides SSN verification, MBR benefit information, and SSR information through a uniform data response based on authorized user-initiated queries. The SVES types are divided into five different responses as follows:

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

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

ATTACHMENT 3 OMITTED

ATTACHMENT 4

ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES

ELECTRONIC INFORMATION EXCHANGE

SECURITY REQUIREMENTS AND PROCEDURES

FOR

STATE AND LOCAL AGENCIES

EXCHANGING ELECTRONIC INFORMATION WITH THE

SOCIAL SECURITY ADMINISTRATION

SENSITIVE DOCUMENT

VERSION 5.0
MARCH 9, 2012

1

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

Table of Contents

ELECTRONIC INFORMATION EXCHANGE
SECURITY REQUIREMENTS AND PROCEDURES
FOR
STATE AND LOCAL AGENCIES
RECEIVING ELECTRONIC INFORMATION FROM THE
SOCIAL SECURITY ADMINISTRATION

1. Introduction Ω

The Social Security Administration (SSA) is required by law to maintain oversight and assure the protection of information it has provided to its *electronic information exchange partners'* (EIEP)s. EIEPs are entities that have established an electronic information sharing agreement with the agency.

The overall aim of this document is twofold. First, to ensure that EIEPs are properly certified as compliant by SSA to SSA security requirements, standards, and procedures expressed in this document, prior to being granted access to SSA information in a production environment; second, to ensure that EIEPs adequately safeguard electronic information provided to them by SSA.

This document (which is considered SENSITIVE by SSA and must be handled accordingly), describes the security requirements which must be met including, SSA's standards and procedures which must be implemented by outside entities (state and local agencies) in order to obtain information from SSA electronically. This document assists outside entities in understanding the criteria that SSA will use when evaluating and certifying the system design, and security features used for electronic access to SSA-provided information. It also provides the framework and general procedures for SSA's security compliance review program intended to ensure, on a periodic basis, conformance to SSA's security requirements by outside entities.

The addition, elimination, and modification of security controls, etc. are predicated upon factors which impact the level of security and due diligence required for mitigating risks, e.g., the emergence of new threats and attack methods, the availability of new security technologies, etc. System security requirements (SSR) are, therefore, periodically reviewed and revised. Accordingly, over time, the SSRs may be subject to change.

The EIEP must comply with SSA's most current SSRs for access to SSA-provided data. However, SSA will work with its partners in the EIEPs' resolution of any deficiencies which occur subsequent to previous approval for access as the result of updated SSRs. Additionally, EIEPs may proactively ensure their ongoing compliance with the SSRs by periodically requesting the most current SSR package from their SSA contact and making such adjustments as may be necessary.

2. Electronic Information Exchange (EIE) Definition Ω

For discussion purposes herein, EIE is any electronic process in which information under SSA control is disclosed to any third party for program or non-program purposes, without the specific consent of the owner of that information. EIE involves individual data transactions and data files that are processed within the programmatic systems of either or all 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 Ω

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

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

b. Social Security Administration (SSA) policies, standards, procedures, and directives.

Privacy information is information about an individual including, but not limited to, personal identifying information including the social security number (SSN).

The data (last 4 digits of the SSN) provided by SSA to its EIEPs for purposes of the Help America Vote Act (HAVA) does not identify a specific individual and, therefore, is not 'Privacy Information' as defined by the Act.

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

Therefore, although the information provided HAVA is not, by definition, 'Privacy Information' and as such, does not require that SSA conduct compliance reviews of entities to which it provides information for purposes of HAVA; SSA does require that those organizations adhere to the terms of their electronic information sharing agreements with SSA.

SSA regional **Data Exchange Coordinators** (DECs) are the bridge between SSA and state EIEPs. As such, in the security arena, DECs will assist OIS in coordinating data exchange security review activities with state and local 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 personally identifiable information (PII).

4. General Systems Security Standards Ω

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

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

a. EIEPs must ensure that means, methods, and technology by which SSA-provided information is processed, maintained, transmitted, or stored neither prevent nor impede the EIEP's ability to:

- safeguard the information in conformance to SSA requirements;

- efficiently investigate fraud, breach, or security events that involve SSA-provided data, or instances of misuse of SSA-provided data.

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

b. EIEPs must ensure that SSA-provided data is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, computer networks, etc. that are located in geographic or virtual areas *not* subject to U.S. law.

c. 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 data are held to the same security requirements as are employees of the EIEP. Refer to the section 'Contractors of Electronic Information Exchange Partners' in the 'Systems Security Requirements' for additional information.

d. Information received from SSA must be stored in a manner that, at all times, is physically and electronically secure from access by unauthorized persons.

e. SSA-provided information must be processed under the immediate supervision and control of authorized personnel.

f. EIEPs must employ both physical and technological safeguards to ensure against unauthorized retrieval of SSA-provided information by means of computer, remote terminal, or other means.

g. EIEPs must have in place formal PII incident response procedures. When faced with a security incident whether caused by malware, unauthorized access, software issues, or acts of nature, etc., EIEP must be able to respond in a manner that protects SSA-provided information affected by the incident.

h. EIEPs must have an active and robust employee security awareness program that is mandatory for all employees who may have access to SSA-provided information.

i. EIEP employees with access to SSA provided 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.

j. At its discretion, SSA or its designee, must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

5. Systems Security Requirements ☊

5.1 Overview ☊

Following is a discussion of SSA's security requirements that must be met by its EIEPs. SSA must certify that controls to meet the requirements have been implemented and working as intended, before it will authorize initiating transactions to and from SSA through batch data exchange processes or online processes such as State Online Query (SOLQ) or Internet SOLQ.

The Systems Security Requirements (SSR)s address management, operational, and technical aspects of security regarding the confidentiality, integrity, and availability of Social Security Administration (SSA) provided information used, maintained, transmitted, or stored by SSA's EIEPs.

SSRs are representative of the current state-of-the-practice security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations and statutes, congressional mandates, etc., including but not limited to the Privacy Act of 1974, the Federal Information Security Management Act (FISMA), etc. and recommended by standards and guidelines established by NIST, etc.

5.2 General System Security Design and Operating Environment ☊

The EIEP must provide descriptions and explanations of their overall system design, configuration, security features, and operational environment and include discussions of how they conform to SSA's requirements. Discussion must also include:

- Description of the operating environment(s) in which SSA-provided data is to be utilized, maintained, and transmitted

- Description of the business process(es) in which SSA-provided information is to be used

- Physical safeguards employed to ensure that unauthorized personnel cannot access SSA-provided data and that audit information pertaining to use of and access to SSA-provided information and the EIEP's associated applications is readily available

- Electronic safeguards, methods, and procedures for protecting the EIEP's network infrastructure and for protecting SSA-provided data while in transit, in use within a process or application, at rest (stored or not in use); preventing 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.)

5.3 System Access Control ☊

EIEPs must utilize and maintain technological (logical) access controls that limit access to SSA-provided information and associated transactions and functions to only those users, processes acting on behalf of authorized users, or devices (including other information systems) authorized for such access based on their official duties or purpose(s). EIEPs must employ a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or a security software design which is *at minimum* equivalent to such products. The access control software must utilize personal identification numbers (PIN) and passwords or

biometric identifiers in combination with the user's system identification code (userID), etc. (e.g., 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 authentication of users).

Depending upon the computing platform (e.g., client/server (PC), mainframe) and the access software implementation, the terms "PIN" and "user system identification code (userID)" may be, for practical purposes, synonymous. For example, the PIN/password combination may be required for access to an individual's PC after which, the userID/password combination may be required for access to a mainframe application. (A biometric identifier may supplant one element in the pair of those combinations).

Implementation of the control software must be in compliance with recognized industry standards. For example, password policies should enforce sufficient construction strength (length and complexity) to defeat or minimize risk-based identified vulnerabilities, ensure limitations for password repetition; technical controls should enforce periodic password changes based on a risk-based standard (e.g., maximum password age of 30 – 45 days, minimum password age of 3 – 7 days), enforce automatic disabling of user accounts that have been inactive for a specified period of time (e.g., 45 days); etc.

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

The EIEPs' systems access rules must cover such matters as least privilege and individual accountability regarding access to sensitive information and associated transactions and functions, control of transactions by permissions modules, the assignment and limitation of system privileges, disabling accounts of separated employees (e.g., within 24 hours), individual accountability, work at home, dial-up access, and connecting to the Internet.

5.4 Automated Audit Trail Ω

EIEPs that receive information electronically from SSA are required to implement and maintain a fully automated audit trail system (ATS). The system must, at a minimum, be capable of creating, storing, protecting, and efficiently retrieving and collecting records identifying the individual user that initiates a request for information from SSA or accesses SSA-provided data. 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 driver license, etc.). Each entry in the audit file must be stored as a separate record, not overlaid by subsequent records. Transaction files must be created to capture all input from interactive internet applications which access or query SSA-provided data.

EIEPs whose transactions with SSA are mediated AND audited by an STC (e.g., State Transmission Component) are responsible for ensuring that the STC's audit capabilities meet SSA's requirements for an automated audit trail system. The EIEP must also establish a process by which the EIEP is able to efficiently obtain audit information from the STC regarding the EIEP's SSA transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Information in the audit file must be retrievable by an automated method and capable of being made available to SSA upon request. Audit trail records must be backed up

on a regular basis to ensure their availability. Backup audit files must have the same level of protection as that applied to the original files.

If SSA-provided information is retained by the EIEP (e.g., Access database, Share Point, etc.), or if certain data elements within the EIEP's system will indicate to users that the information has been verified by SSA, the EIEP's system must also capture an audit trail record of any user who views SSA-provided information stored within the EIEP's system. The audit trail requirements for these inquiry transactions are the same as those outlined above for the EIEP's transactions requesting or accessing information directly from SSA.

5.5 Personally Identifiable Information (PII) 𝛀

PII is defined as any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

PII loss is defined as a circumstance wherein SSA has reason to believe that information on hard copy or in electronic format which contains PII provided by SSA to an EIEP, has left the EIEP's custody or has been disclosed by the EIEP to an unauthorized individual or entity. PII loss is a reportable incident (refer to *Incident Reporting*).

If a PII loss involving SSA-provided data 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 incident (refer to *Incident Reporting*).

5.6 Monitoring and Anomaly Detection 𝛀

The EIEP must establish and/or maintain continuous monitoring of its network infrastructure and assets to ensure that:

- implemented security controls continue to be effective over time

- only authorized individuals, devices, and processes have access to SSA-provided information

- efforts by external and internal entities, devices, or processes to perform unauthorized actions (i.e., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) are detected as soon as they occur

- the necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes

- upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk

- in the event of a data breach or security incident, the necessary remedial actions can be efficiently determined and initiated

- trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are more readily discernable

8

The EIEP's system must include the capability to prevent employees from browsing SSA records (e.g., utilize a permission module and/or employ a system design which is transaction-driven, whereby employees are unable to initiate transactions). If such a design is used, the EIEP then needs only minimal additional monitoring and anomaly detection (detect and monitor employees' attempts to gain access to SSA-provided data to which they are not authorized and attempts to obtain information from SSA for clients not in the EIEP's client system). However, measures must exist to prevent circumvention of the permission module (e.g., creation of a bogus case and subsequently deleting it in such a way that it goes undetected).

If the EIEP's design does not *currently* utilize a permission module *and* is not transaction-driven, until at least one of these security features is implemented, the EIEP must develop and implement compensating security controls to deter 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 transactions or queries requested or initiated by individuals and include systematic or manual procedures for verifying that requests for and queries of SSA-provided information are in compliance with valid official business purposes. The system must also produce reports providing management and/or supervisors with the capability to appropriately monitor user activity, such as:

- User ID Exception Reports:

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

- Inquiry Match Exception Reports:

  This type of report captures information about users who may be initiating transactions for SSNs that have no client case association within the EIEP's system **(100 percent of these cases must be reviewed by the EIEP's management).**

- 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-provided information.

- Inquiry Activity Statistical Reports:

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

The EIEP 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 anomalous activity of users including those who have been granted exceptional system rights and privileges.

5.7 Management Oversight and Quality Assurance Ω

The EIEP must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA-provided information and to ensure that there is ongoing compliance with the terms of the EIEP's

electronic information sharing agreement with SSA and the SSRs established by SSA for access to and use of SSA-provided data by EIEPs. The management oversight function must consist of one or more of the EIEP's management officials whose job functions include responsibility for assuring that access to and use of SSA-provided information is appropriate for each employee position type for which access is granted.

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

Although not required, it is recommended that EIEPs establish the following functions and require that they be performed by employees whose job functions are separate from those who request or use information from SSA:

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

- Random sampling of work activity involving SSA-provided information to determine whether the access and usage comply with SSA's requirements.

5.8 Data and Communications Security 𝛀

EIEPs must encrypt all PII and SSA-provided information when it is transmitted across dedicated communications circuits between its systems, included in intrastate communications among its local office locations, and resident on the EIEP's mobile computers/devices and removable media, etc. The encryption method employed must meet acceptable standards as designated by the National Institute of Standards and Technology (NIST). The recommended encryption method for securing SSA-provided data during transport is the Advanced Encryption Standard (AES) or triple DES (Data Encryption Standard 3) if AES is unavailable. Files encrypted for external users (when using tools such as Microsoft WORD encryption, etc.) require a key length of 9 characters. Although not required, it is recommended that the key (also referred to as a *password*) contain both a number and a special character. However, it is required that the key be delivered in a manner wherein the key does not accompany the media. Also, the key must be secured when unattended or not in use.

It is recommended that the public Internet not be used for transmission of SSA-provided information. If it is, however, Internet and all other electronic communications (e.g., emails and FAXes) containing SSA-provided information must, at minimum, utilize Secure Socket Layer (SSL) and 256-bit encryption protocols or more secure methods such as Virtual Private Network technology. Additionally, the data must be transmitted only to a secure address or device.

EIEPs may retain SSA-provided data for only the business purpose(s) and period of time stipulated in the EIEP's Information Exchange Agreement with SSA. SSA-provided information is to be deleted, purged, destroyed, or returned to SSA when the purpose for which the information was obtained has been completed.

The EIEP may not save or create separate files comprised solely of information provided by SSA. The EIEP may, however, apply specific SSA-provided data to the EIEP's matched record (i.e., specified data obtained from SSA which matches that in the EIEP's preexisting record).

Duplication and redisclosure of SSA-provided information within or outside the EIEP without the written approval of SSA is prohibited.

10

EIEPs must prevent unauthorized disclosure of SSA-provided data after processing has been completed and also after the data is no longer required by the EIEP. The EIEP's operational processes must ensure that no residual SSA-provided data remains on the hard drives of users' workstations after the user has exited the application(s) in which SSA-provided data was utilized. In cases where a PC, hard drive, or other computing or storage device on which SSA-provided information resided will be sent offsite from the EIEP for repair and its information must be retrievable, the EIEP's repair contract must include a requirement for non-disclosure of SSA-provided data by the servicing vendor. SSA-provided information must be completely removed from, rendered unrecoverable, or destroyed on any electronic device or media (e.g., hard drives, removable storage devices, etc.) prior to the device or media being serviced by an external vendor (when the data need not be recovered), excessed, sold, or placed in the custody of another organization.

To sanitize media, one of the following methods must be used:

- **Overwriting**

    Overwrite utilities can only be used on working devices. The media to be overwritten must be designed for multiple reads and writes. This includes disk drives, magnetic tapes, floppies, USB flash drives, etc. The overwrite utility must completely overwrite the media by the *purging* type of media sanitization to make the data irretrievable by a laboratory attack or laboratory forensic procedures (refer to *Definitions* for more information regarding *Media Sanitization*). Reformatting the media does not overwrite the data.

- **Degaussing**

    Degaussing is a sanitization method for magnetic media (e.g., disk drives, tapes, floppies, etc.). Degaussing is not effective for purging non-magnetic media (e.g., optical discs). Degaussing must be performed with a certified tool designed for the media being degaussed. Certification of the tool is required to ensure that the magnetic flux applied to the media is strong enough to render the information irretrievable. The degaussing process must render data on the media irretrievable by a laboratory attack or laboratory forensic procedures (refer to *Definitions* for more information regarding *Media Sanitization*).

- **Physical destruction**

    Physical destruction is the method which must be used 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 data in hardcopy if it is required to fulfill evidentiary requirements, provided the agencies retire such data in accordance with applicable state laws governing state agencies' retention of records. The EIEP must ensure that print media containing SSA-provided data is controlled to restrict its access to only authorized employees who need such access to perform their official duties and must have in place secure processes by which print media containing SSA-provided data is destroyed when it is no longer required. Paper documents containing SSA-provided data must be destroyed by burning, pulping, shredding, macerating, or other similar means that ensures that the information cannot be recovered.

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.

5.9 Incident Reporting Ω

The EIEP must develop and implement policies and procedures for responding to the breach or loss of PII and explain how they conform to SSA's requirements. The procedures must include the following information:

*If the EIEP experiences or suspects a breach or loss of PII or a security incident which includes SSA-provided data, they must notify the United States Computer Emergency Readiness Team (US-CERT) **within one hour** of discovering the incident. The EIEP must also notify the SSA Systems Security contact named in the agreement. If within 1 hour the EIEP has been unable to make contact with that person, the EIEP must call 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, **Attachment 5,** provided in the agreement to facilitate gathering and organizing information about an incident.*

The EIEP must agree that if SSA determines that the risk presented by the breach or security incident requires the notification of the individuals whose information is involved and/or remedial action, the EIEP will perform those actions without cost to SSA.

5.10 Security Awareness and Employee Sanctions Ω

The EIEP must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees granted access to SSA-provided information. Training must include discussion of:

- 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 of and security in systems processing SSA-provided data

- Restrictions on viewing and/or copying SSA-provided information

- The employees' responsibility for proper use and protection of SSA-provided information including its proper disposal

- Security incident reporting procedures

- The possible sanctions and penalties for misuse of SSA-provided information.

The EIEP must provide security awareness training periodically or as needed, and have in place administrative procedures for sanctioning employees who violate laws governing the use and misuse of SSA-provided data through unauthorized or unlawful use or disclosure of SSA-provided information.

5.11 Contractors of Electronic Information Exchange Partners Ω

As previously stated, in **_The General Systems Security Standards_**, contractors of the EIEP are held to the same security requirements as are employees of the EIEP. As such, the EIEP is responsible for oversight and compliance of their contractors with SSA's security requirements. The EIEP must be able to provide proof of the contractual agreement between itself and its contractors (e.g., copy of their contract, etc.) who are authorized by the EIEP to perform on its behalf and who have access to or are involved in the processing, handling, transmission, etc. of information provided to the EIEP by SSA. The EIEP must also explain the role of those contractors within the EIEP's operations.

The EIEP must also require that their contractors who will have access to or be involved in the processing, handling, transmission, etc. of information provided to the EIEP by SSA, sign an agreement with the EIEP that obligates the contractor to follow the terms of the EIEP's data exchange agreement with SSA. The EIEP must provide its contractors a copy of the data exchange agreement between the EIEP and SSA and related attachments before any disclosure by the EIEP of SSA-provided information to the EIEP's contractor/agent.

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

- safeguards for sensitive information

- computer system safeguards

- security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and redisclosure of SSA-provided information

6. General -- Security Certification and Compliance Review Programs Ω

SSA's security certification and compliance review programs are two distinct programs with the same objective. The certification program is a one-time process associated exclusively with an EIEP's initial request for electronic access to SSA-provided information or an initial change to online access. The certification process entails two rigorous stages intended to ensure that technical, management, and operational security measures implemented by EIEPs fully conform to SSA's security requirements and are working as intended. EIEPs must satisfy both stages of the certification process before SSA will permit online access to its data in a production environment.

The compliance review program, however, is intended to ensure that the suite of security measures implemented by an EIEP to safeguard SSA-provided data remains in full compliance with SSA's security standards and requirements. The compliance review program is applicable to online access to SSA-provided data as well as batch processes. Under the compliance review program, EIEPs are subject to ongoing periodic security reviews by SSA that are regularly scheduled or ad hoc.

6.1 The Security Certification Program Ω

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

- Phase One: The Security Design Plan (SDP) phase wherein a formal written plan is authored by the EIEP to comprehensively document its technical and non-technical

security controls to safeguard SSA-provided information (refer to _**Documenting Security Controls in the Security Design Plan**_).

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

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

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

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

6.2.1 When the SDP and RA are Required Ω

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

- to obtain approval for requested initial access to SSA-provided information for an initial agreement

- to obtain approval to reestablish previously terminated access to SSA-provided data

- when implementing a new operating or security platform in which SSA-provided data will be involved

- significant changes to the EIEP's organizational structure, technical processes, operational environment, data recovery capabilities, or security implementations are planned or have been made since approval of their most recent SDP or of their most recent successfully completed security review

- one or more security breaches or incidents involving SSA-provided data have occurred since approval of the EIEP's most recent SDP or of their most recent successfully completed security review

- to document descriptions and explanations of measures implemented as the result of a data breach or security incident

- to document descriptions and explanations of measures implemented to resolve non-compliancy issue(s)

- when approval of the SDP has been revoked

The RA may also be required if changes (other than those listed above) that may impact the terms of the EIEP's data sharing agreement with SSA have occurred.

The SDP must be approved by SSA prior to the initiation of transactions and/or access to SSA-provided information by the EIEP.

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

Deficiencies identified through the evaluation of the SDP must be corrected by the EIEP and a revised SDP which incorporates descriptions and explanations of the measures implemented to eliminate the deficiencies must be submitted. Until the deficiencies have been corrected and documented in its SDP, and the SDP is approved, the EIEP will not be granted access to SSA-provided information or certified for electronic receipt of the information. The progress of corrective implementation(s) must be communicated to SSA on a regular basis. If, within a reasonable time as determined by SSA, the EIEP is unable to rectify a deficiency determined by SSA to present an untenable risk to SSA-provided information or the agency, approval of the SDP will be withheld.

If, at any time subsequent to approval of its SDP the EIEP is found to be in non-compliance with one or more SSRs, SSA may revoke approval of the EIEP's access to SSA-provided data. A revised SDP which incorporates descriptions and explanations of the measures implemented to resolve the non-compliance issue(s) must be submitted. The progress of corrective implementation(s) must be communicated to SSA on a regular basis. Until resolution of the issue(s) has been accomplished and documented in its SDP, and the SDP is approved, the EIEP will be in non-compliance with SSA's SSRs. If, within a reasonable time as determined by SSA, the EIEP is unable to rectify a deficiency determined by SSA to present an untenable risk to SSA-provided information or to SSA, approval of the SDP will be withheld and the flow of SSA-provided information to the EIEP may be discontinued.

NOTE: EIEPs that function only as an STC, transferring SSA-provided data to other EIEPs must, per the terms of their agreements with SSA, adhere to SSA's System Security Requirements (SSR) and exercise their responsibilities regarding protection of SSA-provided information.

6.3 The Certification Process Ω

Once the EIEP has successfully satisfied Phase 1, SSA will conduct an onsite certification review. The objective of the onsite review will be to ensure by SSA's examination and the EIEP's demonstration that the non-technical and technical controls implemented by the EIEP to safeguard Social Security-provided data from misuse and improper disclosure are fully functioning and working as intended.

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

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

- a demonstration of the EIEP's implementation of each requirement

- random sampling of audit records and transactions submitted to SSA

- a walkthrough of the EIEP's data center to observe and document physical security safeguards

- a demonstration of the EIEP's implementation of electronic exchange of data with SSA

- discussions with managers/supervisors

- examination of management control procedures and reports (e.g., anomaly detection reports, etc.)

- demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention, specifically:

  o If the design is based on a permission module or similar design, or is transaction driven, the EIEP will demonstrate how the system triggers requests for information from SSA.

  o If the design is based on a permission module, the EIEP will demonstrate the process by which requests for SSA-provided information are prevented for SSNs not present in the EIEP's system (e.g.; by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEP's system).
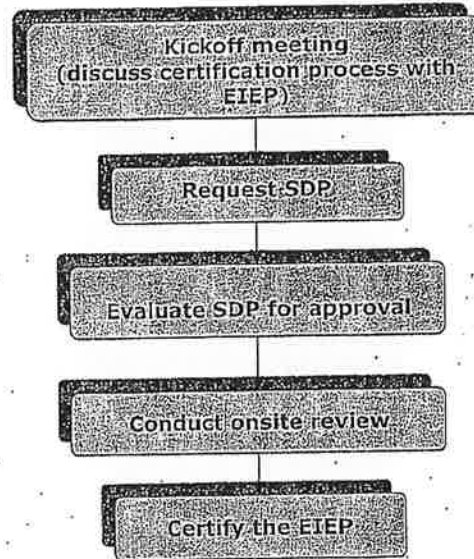
During the certification review, SSA, or a certifier acting on its behalf, may request a demonstration of the system's audit trail and retrieval capability. The certifier may request a demonstration of the system's capability for tracking the activity of employees that are permitted to view SSA-provided information within the EIEP's system. Additionally, the certifier may request those EIEPs whose transactions with SSA are mediated AND audited by an STC to demonstrate the process(es) by which the EIEP obtains audit information from the STC regarding the EIEP's SSA transactions.

EIEPs whose transactions with SSA are mediated AND audited by an STC will be required to demonstrate both their own in-house audit capabilities AND the process(es) by which the EIEP obtains audit information from the STC regarding the EIEP's transactions with SSA.

If the EIEP employs a contractor who will be involved with the processing, handling, transmission, etc. of the EIEP's SSA-provided information offsite from the EIEP, SSA, at its discretion, may include in the onsite certification review an onsite inspection of the contractor's facility. The inspection may occur with or without a representative of the EIEP.

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

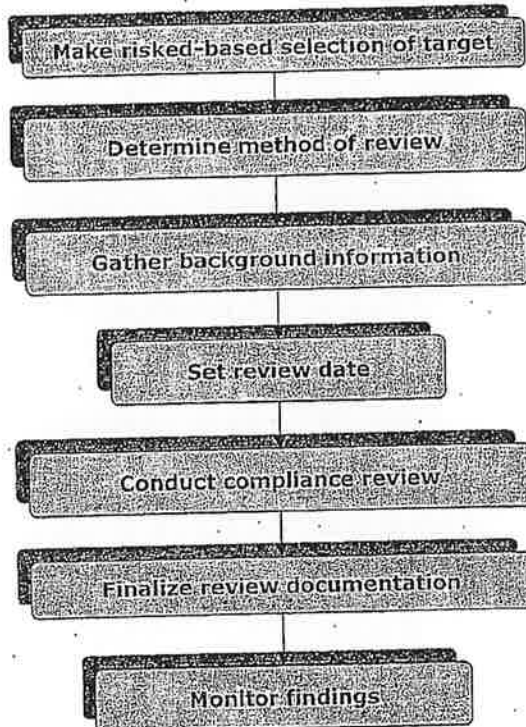The following is a high-level flow chart of the OIS Certification Process: Ω

```
┌─────────────────────────────────┐
│         Kickoff meeting          │
│  (discuss certification process  │
│           with EIEP)             │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│           Request SDP            │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│      Evaluate SDP for approval   │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│        Conduct onsite review     │
└─────────────────────────────────┘
                 │
┌─────────────────────────────────┐
│          Certify the EIEP        │
└─────────────────────────────────┘
```

6.5   The Compliance Review Program and Process   Ω

Similar to the certification process, the compliance review program entails a rigorous process. intended to ensure that EIEPs currently receiving electronic information from SSA are in full compliance with the Agency's security requirements and standards. As a practice, SSA attempts to conduct compliance reviews following a 3 to 5 year periodic review schedule. However, as circumstances warrant, a review may take place at anytime. Three prominent examples that would trigger an ad hoc review are:

- a significant change in the outside EIEP's computing platform

- a violation of any of SSA's systems security requirements

- an unauthorized disclosure of SSA information by the EIEP

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

Make risked-based selection of target

Determine method of review

Gather background information

Set review date

Conduct compliance review

Finalize review documentation

Monitor findings

SSA may, at its discretion, conduct compliance reviews onsite at the EIEPs' site, including a field office location, if appropriate.

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

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

- a demonstration of the EIEP's implementation of each requirement

- random sampling of audit records and transactions submitted to SSA

- a walkthrough of the EIEP's data center to observe and document physical security safeguards

- a demonstration of the EIEP's implementation of online exchange of data with SSA

- discussions with managers/supervisors

- examination of management control procedures and reports (e.g., anomaly detection reports, etc.)

- demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention, specifically:

  o If the design is based on a permission module or similar design, or is transaction driven, the EIEP will demonstrate how the system triggers requests for information from SSA.

  o If the design is based on a permission module, the EIEP will demonstrate the process by which requests for SSA-provided information are prevented for SSNs not present in the EIEP's system (e.g.; by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEP's system).

SSA may also, at its discretion, perform an ad hoc onsite or remote review for reasons including but not limited to the following:

- the EIEP has experienced a security breach or incident involving SSA-provided data

- the EIEP has unresolved non-compliancy issue(s)

- to review an EIEP's offsite (relative to the EIEP) contractor's facilities involving SSA-provided data

- the EIEP is a legacy organization that has not yet been through SSA's security certification and compliance review programs

- the EIEP has requested that an IV & V (Independent Verification and Validation review) be performed by SSA

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 that are permitted to view SSA-provided information within the EIEP's system. Additionally, the certifier may request those EIEPs whose transactions with SSA are mediated AND audited by an STC to demonstrate the process(es) by which the EIEP obtains audit information from the STC regarding the EIEP's SSA transactions.

EIEPs whose transactions with SSA are mediated AND audited by an STC may be required to demonstrate both their own in-house audit capabilities AND the process(es) by which the EIEP obtains audit information from the STC regarding the EIEP's transactions with SSA.

If the EIEP employs a contractor who will be involved with the processing, handling, transmission, etc. of the EIEP's SSA-provided information offsite from the EIEP, SSA, at its discretion, may include in the onsite compliance review an onsite inspection of the contractor's facility. The inspection may occur with or without a representative of the EIEP. However, manpower limitations or fiscal constraints could drive an alternative approach, such as teleconferencing. In any event, the format of the review in routine circumstances (i.e., the compliance review is not being conducted to address a special circumstance, such as a disclosure violation, 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. Findings and recommendations from SSA's compliance review; if any, will be discussed in its report and monitored for closure.

NOTE: Documentation provided SSA by the EIEP for compliance reviews is considered sensitive and is, therefore, handled accordingly by SSA. E.g., the information is accessible to only authorized individuals who have a need for the information as it relates to compliance of the EIEP with its electronic information sharing agreement with SSA and SSA's associated system security requirements and procedures. Additionally, the EIEP's documentation is retained for only as long as required and is deleted, purged, or destroyed when the requirement for which the information was obtained has expired.

The following is a high-level example of the analysis that aids in making preliminary decisions as to which review format may be most appropriate. Various additional factors may also be factored in determining whether SSA performs an onsite or remote compliance review.

- High/Medium Risk Criteria
  - undocumented closing of prior review finding(s)
  - implementation of technical/operational controls that impact security of SSA provided data (e.g., implementation of new data access method, etc.)
  - reported PII breach

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

6.5.1 EIEP Compliance Review Participation Ω

During the compliance review SSA may request to meet with the following:

- a sample of managers and/or supervisors responsible for enforcing and monitoring ongoing compliance to security requirements and procedures to assess their level of training to monitor their employee's use of SSA-provided information, and for reviewing reports and taking necessary action

- the individuals responsible for security awareness and employee sanction functions and request an explanation of how these responsibilities are performed

- a sample of the EIEP's employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA-provided information

- the individual(s) responsible for management oversight and quality assurance functions and request a description of how these responsibilities will be carried out

- additional individuals as deemed appropriate by SSA

6.5.2 Verification of Audit Samples Ω

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

The EIEP must provide SSA a written attestation of the results of the EIEP's review of the transactions. The document must provide:

- confirmation for each sample transaction located in the EIEP's audit file(s) and determined to have been submitted by its employee(s) for legitimate and authorized business purposes

- an explanation for each sample transaction located in the EIEP's audit file(s) determined to have been unauthorized

- an explanation for each sample transaction not found in the EIEP's ATS

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

6.6 Scheduling the Onsite Review ⋒

The SDP must be approved before its associated onsite review is scheduled. Notification of the approval of a plan will be sent via email. Although there is no prescribed time frame for arranging the subsequent onsite review (*certification review* for an EIEP requesting initial access to SSA-provided information for an initial agreement or *compliance review* for other EIEPs), unless there are compelling circumstances precluding it, the onsite review will follow as soon as reasonably possible.

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

- the reason for submission of a plan

- the severity of security issues if any

- circumstances of the previous review if any

- SSA workload considerations

Although the scheduling of the review is contingent upon approval of the SDP, in extreme circumstances, SSA may, at its discretion, perform an onsite review prior to approval if determined necessary by SSA for completion of the evaluation of a plan.

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

21

7. Additional Definitions Ω

Back Button:
Refers to a button on a web browser's toolbar, the *backspace button* on a computer keyboard, a programmed keyboard button or mouse button, etc., that returns a user to a previously visited web page or application screen.

Breach:
Refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording.

Browsing:
Requests for or queries of SSA-provided data for purposes not related to the performance of official job duties.

Choke Point:
The firewall between a local network and the Internet is considered a choke point in network security, because any attacker would have to come through that channel, which is typically protected and monitored.

Cloud Computing:
The term refers to Internet-based computing and is derived from the cloud drawing representing the Internet in computer network diagrams. Cloud computing providers deliver on-demand online computing resources (e.g., services, software applications, data storage, and information) accessible to their customers by means of a web service or browser.

Cloud Drive:
A cloud drive is a Web-based service that provides storage space on a remote server.

CloudAudit:
CloudAudit is a specification that provides cloud computing service providers a standard way to present and share detailed, automated statistics about performance and security.

Commingling:
The process by which an EIEP adjoins specific SSA-provided data to specific preexisting EIEP information according to a particular data-matching scheme.

Degaussing:
Degaussing is the method of using a degausser (i.e., a device that generates a magnetic field) in order to disrupt magentically recorded information. Degaussing can be effective for purging damaged media and media with exceptionally large storage capacities. Degaussing is not effective for purging non-magnetic media (e.g., optical discs).

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

Function:
One or more persons or organizational components assigned to serve a particular purpose, or perform a particular role. Also, the purpose, activity, or role assigned to one or more persons or organizational components.

Hub:
As it relates to electronic data exchange with SSA, a hub is an organization which performs as an electronic information distribution and/or collection point (and may also be referred to as a State Transmission Component or STC).

ICON:
Interstate Connection Network (various entities use 'Connectivity' rather than 'Connection')

IV & V:
Independent Verification and Validation

Legacy System:
A term usually referring to a corporate or organizational computer system or network that utilizes outmoded programming languages, software, and/or hardware that typically no longer receive support from the original vendors or developers.

Manual Transaction:
An operation (also referred to as a 'user-initiated transaction') which is initiated at the volition of a user rather than system-generated within an automated process.

Example: A user enters a client's information including the client's SSN on an input screen and presses the 'ENTER' key to acknowledge that input of data has been completed. A new screen appears with multiple options which include 'VERIFY SSN' and 'CONTINUE'. The user has the option to verify the client's SSN or perform alternative actions.

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

- Clearing: This type of media sanitization is considered to be adequate for protecting information from a robust keyboard attack. Clearing must prevent retrieval of information by data, disk, or file recovery utilities. Clearing must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. Deleting items, however, is not sufficient for clearing.

  This process may include overwriting all addressable locations of the data, as well as its logical storage location (e.g., its file allocation table). The aim of the overwriting process is to replace or obfuscate existing information with random data. Most rewriteable media may be cleared by a single overwrite. This method of sanitization cannot be utilized on unwriteable or damaged media.

- Purging: This type of media sanitization is a process that protects information from a laboratory attack. The terms clearing and purging are sometimes considered synonymous. However, for some media, clearing is not sufficient for purging (i.e., protecting data from a laboratory attack). Although most rewriteable media may be cleared by a single overwrite, purging may require multiple rewrites using different characters for each write cycle.

  This is because a laboratory attack involves threats with the capability to employ non-standard assets (e.g., specialized hardware) to attempt data recovery on media outside of that media's normal operating environment.

  Degaussing is also an example of an acceptable method for purging magnetic media. If purging media is not a viable method for sanitization, the media should be destroyed.

- Destruction: Physical destruction of media is the most effective form of sanitization. Methods of destruction include burning, pulverizing, and shredding. Any residual medium should be able to withstand a laboratory attack.

Permission module:

A utility or subprogram within an application which automatically enforces the relationship of a request for or query of SSA-provided data to an authorized process or transaction legitimately initiated; e.g., verification of an SSN for issuance of a driver license which can be triggered only automatically from within a state's driver license application, requests for information from SSA by an EIEP's employee which cannot be initiated unless the EIEP's client system has a record containing the SSN of the individual for which information is sought, etc.

Screen Scraping:

Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This was generally done by reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is also commonly used to refer to the bidirectional exchange of data.

A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

Security Breach:

An act from outside an organization that bypasses or contravenes security policies, practices, or procedures.

Security Incident:

A fact or event which signifies the possibility that a breach of security may be taking place, or may have taken place. All threats are security incidents, but not all security incidents are threats.

Security Violation:

An act from within an organization that bypasses or contravenes security policies, practices, or procedures.

Sensitive data:

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

SMDS (Switched Multimegabit Data Service (SMDS):
SMDS is a telecommunications service that provides connectionless, high- performance, packet-switched data transport. Although not a protocol, it supports standard protocols and communications interfaces using current technology.

SSA-provided data/information:
Synonymous with 'SSA-supplied data/information', defines information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. The following are examples of SSA-provided data/information information:

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)

- SSA's response to a query from an EIEP for verification of an SSN

SSA data/information:
This is term, sometimes used interchangeably with 'SSA-provided data/information', denotes information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. However, **'SSA data/information'** also includes information provided to the EIEP by a source other than SSA, but which is attested by the EIEP to have been verified by SSA, or is coupled with data from SSA as to the accuracy of the information. The following are examples of SSA information:

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)

- SSA's response to a query from an EIEP for verification of an SSN

- Display by the EIEP of SSA's response to a query for verification of an SSN **and** the associated SSN provided by SSA

- Display by the EIEP of SSA's response to a query for verification of an SSN **and** the associated SSN provided to the EIEP by a source other than SSA

- Electronic records that contain only SSA's response to a query for verification of an SSN **and** the associated SSN whether provided to the EIEP by SSA or a source other than SSA

SSN:
Social Security Number

STC:
A State Transmission Component is an organization which performs as an electronic information distribution and/or collection point for one or more other entities (and may also be referred to as a hub).

System-generated transaction:
A transaction automatically triggered by an automated system process.

Example: A user enters a client's information including the client's SSN on an input screen and presses the 'ENTER' key to acknowledge that input of data has been completed. An automated process then matches the SSN against the user's organization's database and when no match is found, automatically sends an electronic request for verification of the SSN to SSA.

Systems process:
Refers to a software program module that runs in the background within an automated batch, online, or other process.

Third Party:
This term pertains to an entity (person or organization) provided access to SSA-provided information by an EIEP or other SSA business partner for which one or more of the following apply:
- is not stipulated access to SSA-provided data by an information-sharing agreement between an EIEP and SSA
- has no information-sharing agreement with SSA
- is not directly authorized by SSA for access to SSA-provided data

Transaction-driven:
This term pertains to an automatically initiated online query of or request for SSA Information by an automated transaction process (e.g., driver license issuance, etc.). The query or request will only occur if prescribed conditions are met within the automated process.

Uncontrolled transaction:
This term pertains to a transaction that is not controlled by a permission module (i.e., not subject to a systematically enforced relationship to an authorized process or application or an existing client record).

8. Regulatory References Ω

Federal Information Processing Standards (FIPS) Publications

Federal Information Security Management Act of 2002 (FISMA)

Homeland Security Presidential Directive (HSPD-12)

National Institute of Standards and Technology (NIST) Special Publications

Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*

Office of Management and Budget (OMB) Circular A-130, Appendix III, *Management of Federal Information Resources*

Office of Management and Budget (OMB) Memo M-06-16, *Protection of Sensitive Agency Information, June 23, 2006*

Office of Management and Budget (OMB) Memo M-07-16, *Memorandum for the Heads of Executive Departments and Agencies, May 22, 2007*

Office of Management and Budget (OMB) Memo M-07-17, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007*

Privacy Act of 1974

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

1. Q: What is a breach of data?
   A: Refer also to Security Breach, Security Incident, and Security Violation.

2. Q: What is employee browsing?
   A: Click hyperlink

3. Q: Okay, so the SDP was submitted. Can the Onsite Review be scheduled now?
   A: Refer to Scheduling the Onsite Review.

4. Q: What is a 'Permission Module'?
   A: Click hyperlink

5. Q: What is meant by Screen Scraping?
   A: Click hyperlink

6. Q: When does an SDP have to be submitted?
   A: Refer to When the SDP and RA are Required.

7. Q: Does an SDP have to be submitted when the agreement is renewed?
   A: The SDP does not have to be submitted **because** the agreement between the EIEP and SSA was renewed. There are, however, circumstances that require an SDP to be submitted. Refer to When the SDP and RA are Required.

8. Q: Is it acceptable to save SSA data with a verified indicator on a (EIEP) workstation as long as the hard drive is encrypted? If not, what options does the agency have?
   A: There is no problem with an EIEP saving SSA-provided information to the encrypted hard drives of computers processing the data provided the information is retained only as provided for in the EIEP's data-sharing agreement with SSA. Refer to Data and Communications Security.

9. Q: Is caching of SSA-provided data on EIEP workstations allowed?
   A: Caching during processing is not a problem. However, SSA-provided data must be cleared from the cache when the user exits the application in which the data was used or accessed. Refer to Data and Communications Security.

10. Q: What is meant by "Interconnections to other systems"?
    A: As used in SSA's system security requirements document, the term "interconnections" is synonymous with "connections".

11. Q: Is it acceptable to submit the SDP as a PDF file?
    A: No, it is not.

12. Q: Should the SDP be written from the standpoint of my agency's SVES access itself, or from the standpoint of access to all data provided to us by SSA?
    A: The SDP is to encompass your agency's electronic access to SSA-provided data as per the electronic data sharing agreement between your agency and SSA. Refer to Developing the SDP.

15. Q: Does having a "transaction-driven" system mean that employees cannot initiate a query to SSA and that a permission module is not needed?
    A: Not necessarily. "Transaction driven" basically means that queries, etc. are submitted automatically (and it might depend on the transaction). Depending on the system

implementation, queries might not be automatic or, if they are, manual transactions might still be permitted (for example, when something needs to be corrected). Also, even if a "transaction-driven" system is implemented in such a way that manual transactions cannot be performed, if the system does **not** require the user to be in a particular application and/or the query to be for an existing record in the EIEP's system **before** the system will allow a query to go through to SSA, it would still need a permission module.

16. Q: What is an Onsite Compliance Review?
A: The Onsite Compliance Review is the process wherein SSA performs periodic site visits to its Electronic Information Exchange Partners (EIEP) to certify whether the EIEP's technical, managerial, and operational security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEPs' data sharing agreements with SSA and SSA's associated system security requirements and procedures. Refer to the Compliance Review Program and Process.

17. Q: What are the criteria for performing an Onsite Compliance Review?
A: The following are criteria for performing the Onsite Compliance Review:

- EIEP initiating new access or new access method for obtaining information from SSA

- EIEP's cyclical review (previous review was performed remotely)

- EIEP has made significant change(s) in its operating or security platform involving SSA-provided data

- EIEP experienced a breach of SSA-provided personally identifying information (PII)

- EIEP has been determined to be high-risk

Refer also to the Review Determination Matrix.

18. Q: What is a Remote Compliance Review?
A: The Remote Compliance Review is the process wherein SSA conducts periodic meetings remotely (e.g., via conference calls) with its EIEPs to determine whether the EIEP's technical, managerial, and operational security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEPs' data sharing agreements with SSA and SSA's associated system security requirements and procedures. Refer to the Compliance Review Program and Process.

19. Q: What are the criteria for performing a Remote Compliance Review?
A: Each of the following criteria must be satisfied for performing the Remote Compliance Review:

- EIEP's cyclical review (previous review was performed onsite without findings or issues for which findings were cited have been satisfactorily resolved).

- EIEP has made no significant change(s) in its operating or security platform involving SSA-provided data.

- EIEP has not experienced a breach of SSA-provided personally identifying information (PII) since its previous compliance review.

- EIEP has been determined to be low-risk

Refer also to the Review Determination Matrix

29

(This page blank)

Ω

ATTACHMENT 5

WORKSHEET FOR REPORTING LOSS OR POTENTIAL LOSS OF PERSONALLY IDENTIFABLE INFORMATION

ATTACHMENT 5

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable
Information

1. Information about the individual making the report to the NCSC:

Name:				
Position:				
Deputy Commissioner Level Organization:				
Phone Numbers:				
Work:		Cell:		Home/Other:
E-mail Address:				
Check one of the following:				
Management Official		Security Officer		Non-Management

2. Information about the data that was lost/stolen:
   Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

Name		Bank Account Info	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Info	
Place of Birth		Mother's Maiden Name	
Address		Other (describe):	

   Estimated volume of records involved:

3. How was the data physically stored, packaged and/or contained?
Paper or Electronic? (circle one):

If Electronic, what type of device?

Laptop		Tablet		Backup Tape		Blackberry	
Workstation		Server		CD/DVD		Blackberry Phone #	
Hard Drive		Floppy Disk		USB Drive			
Other (describe):							

Additional Questions if Electronic:

	Yes	No	Not Sure
a. Was the device encrypted?			
b. Was the device password protected?			
c. If a laptop or tablet, was a VPN SmartCard lost?			
Cardholder's Name:			
Cardholder's SSA logon PIN:			
Hardware Make/Model:			
Hardware Serial Number:			

Additional Questions if Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted?			
e. Other circumstances:			

4. If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NCSC (as listed in #1), information about this employee/contractor:

Name:	
Position:	
Deputy Commissioner Level Organization:	
Phone Numbers:	
Work:	Cell:	Home/Other:
E-mail Address:	

5. Circumstances of the loss:
   a. When was it lost/stolen?

   b. Brief description of how the loss/theft occurred:

   c. When was it reported to SSA management official (date and time)?

6. Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)

7. Which reports have been filed? (include FPS, local police, and SSA reports)

Report Filed	Yes	No	Report Number		
Federal Protective Service					
Local Police					
				Yes	No
SSA-3114 (Incident Alert)					
SSA-342 (Report of Survey)					
Other (describe)					

8. Other pertinent information (include actions under way, as well as any contacts with other agencies, law enforcement or the press):

RECERTIFICATION OF THE COMPUTER MATCHING AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE HEALTH AND HUMAN SERVICES AGENCY OF CALIFORNIA
(STATE AGENCY)

SSA Match #6003

Under the applicable provisions of the Privacy Act of 1974, amended by the Computer Matching and Privacy Protection Act (CMPPA) of 1988, 5 U.S.C. § 552a(o)(2), a computer matching agreement will remain in effect for a period not to exceed 18 months. Within 3 months prior to the expiration of such computer matching agreement, however, the Data Integrity Board (DIB) may, without additional review, renew the computer matching agreement for a current, ongoing matching program for a period not to exceed 12 additional months if:

1. such program will be conducted without any changes; and

2. each party to the agreement certifies to the DIB in writing that the program has been conducted in compliance with the agreement.

The following match meets the conditions for renewal by this recertification:

I. TITLE OF MATCH:

Computer Matching and Privacy Protection Act Agreement Between the Social Security Administration and the Health and Human Services Agency of California (Match #6003)

II. PARTIES TO THE MATCH:

Recipient Agency: The Health and Human Services of California (State Agency)

Source Agency: Social Security Administration (SSA)

III. PURPOSE OF THE AGREEMENT:

This CMPPA Agreement between SSA and the State Agency, sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein "data") made by SSA to the State Agency that administers federally funded benefit programs under various provisions of the Social Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), including the state-funded state supplementary payment programs under title XVI of the Act. 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 for state benefits from SSA Privacy Act Systems of Records and verifies the Social Security numbers of the applicants.

IV. ORIGINAL EFFECTIVE AND EXPIRATION DATES OF THE MATCH:

Effective Date: July 1, 2012
Expiration Date: December 31, 2013

V. RENEWAL AND NEW EXPIRATION DATES:

Renewal Date: January 1, 2014
New Expiration Date: December 31, 2014

VI. CHANGES:

By this recertification, SSA and the State Agency make the following non-substantive changes to the computer matching agreement:
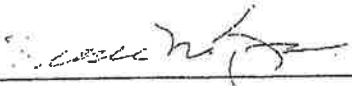
In Article XIV, "Points of Contact," information under subsection A., "SSA Point of Contact, Regional Office," should be deleted in its entirety and replaced with the following:

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

Social Security Administration

Source Agency Certification:

As the authorized representative of the source agency named above, I certify that: (1) the subject matching program was conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any change for an additional 12 months, subject to the approval of the Data Integrity Board of the Social Security Administration.

Grace M. Kim
Regional Commissioner
San Francisco

Date_____

Data Integrity Board Certification:

As Chair of the Data Integrity Board of the source agency named above, I certify that: (1) the subject matching program was conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any change for an additional 12 months.
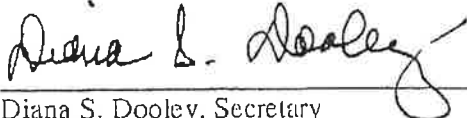
Kirsten J. Moncada
Chair
Data Integrity Board

Date___ 7/10/12

Health and Human Services Agency of California

Recipient Agency Certification:

As the authorized representative of the recipient agency named above, I certify that:
(1) the subject matching program was conducted in compliance with the existing
computer matching agreement between the parties; and (2) the subject matching program
will continue without any change for an additional 12 months, subject to the approval of
the Data Integrity Board of the Social Security Administration.

Diana S. Dooley, Secretary

Date October 30, 2013