AGENDA ITEM NO.
D-12

COUNTY OF HUMBOLDT

For the meeting of: September 16, 2008

Date: August 19, 2008

To: Board of Supervisors

From: Phillip R. Crandall, Director,
Department of Health and Human Services

Subject: Approval Medi-Cal Data Privacy and Security Agreement with the California Department of Health Care Services

RECOMMENDATIONS:

That the Board of Supervisors:

1. Approve Medi-Cal Data Privacy and Security Agreement with the California Department of Health Services; and

2. Authorize the Director of the Social Services Branch to sign two (2) copies the Agreement.

SOURCE OF FUNDING:

Social Services Branch Allocations. (Budget Unit 511).

Prepared by Mark Magladry Administrative Analyst CAO Approval Phillip Smith Hanes

REVIEW:
Auditor _____ County Counsel [signature] Personnel _____ Risk Manager [signature] Other _____

TYPE OF ITEM:
__X__ Consent
_____ Departmental
_____ Public Hearing
_____ Other _____

PREVIOUS ACTION/REFERRAL:

Board Order No. _____

Meeting of: _____

BOARD OF SUPERVISORS, COUNTY OF HUMBOLDT
Upon motion of Supervisor WOOLLEY
Seconded by Supervisor NEELY
And unanimously carried by those members present,
The Board hereby adopts the recommended action
contained in this report.

Dated: September 16, 2008
Kathy Hayes, Clerk of the Board
By: Vikki Turner

DISCUSSION:

The California Department of Health Care Services (DHCS) has proposed a Medi-Cal Data Privacy and Security Agreement to ensure the privacy and security of Medi-Cal Personally Identifiable Information. DHCS receives federal funding to administer the Medi-Cal program, which provides funding to the Humboldt County Department of Health and Human Services in exchange for the Department's assistance in administering the Medi-Cal program.

The agreement covers county workers that assist in the administration of the Medi-Cal program, and who access, use and disclose Medi-Cal Personally Identifiable Information. County staff will obtain Medi-Cal Personally Identifiable Information when performing the administrative function of Medi-Cal. Medi-Cal Personally Identifiable Information consist of any information used to identify an individual, including a person's name, social security number, date of birth, driver's license number, or identification number. Under the terms of this Agreement, county staff may use or disclose this information only to perform functions, activities or services directly related to the administration of the Medi-Cal program.

Staff will be trained on the requirements of the Agreement to safeguard this information. The Department will train all new employees within 30 days of employment and will provide ongoing reminders on the privacy and security requirements. The Department's management will establish and maintain ongoing oversight for monitoring workforce compliance.

The Department also agrees to ensure that all Medi-Cal Personally Identifiable Information is physically safe from access by unauthorized persons and will comply with the computer security safeguards outlined in the Agreement. County Welfare Directors Association (CWDA) aided California counties in negotiating this Agreement with DHCS.

At this time, the Department request authorization from the Board of Supervisors to have the Director of the Social Services Branch sign two copies of the Agreement.

FINANCIAL IMPACT:

The security guidelines of the Agreement require improvements with physical and electronic safeguards, such as locks, and filing cabinets, as well as the acquisition of an electronic encryption tool. Fiscal year 2008-2009 Department of Health and Human Services funding will be used for the procurement of these improvements with no financial impact to the General Fund.

OTHER AGENCY INVOLVEMENT:

County Welfare Directors Association (CWDA)

ALTERNATIVES TO STAFF RECOMMENDATIONS:

The Board of Supervisors can choose not to approve the agreement. The California Department of Health Care Services (DHCS) is expecting that counties approve the Agreement.

ATTACHMENT:

Exhibit A: Agreement between the Social Security Administration and the State of California, Department of Health Care Services with Attachment "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration".

MEDI-CAL DATA PRIVACY AND SECURITY AGREEMENT BETWEEN The California Department of Health Care Services and the County of Humboldt, Department of Health and Human Services

PREAMBLE

The California Department of Health Care Services (DHCS) and the County of Humboldt, Department of Health and Human Services ("County Department") enter into this Medi-Cal Data Privacy and Security Agreement ("Agreement") in order to ensure the privacy and security of Medi-Cal Personally Identifiable Information (PII).

DHCS receives federal funding to administer the Medi-Cal program. DHCS provides funding to the County Department in exchange for the County Department's assistance in administering the Medi-Cal program.

This Agreement covers the County of Humboldt, Department of Health and Human Services workers that assist in the administration of the Medi-Cal program; and access, use, or disclose Medi-Cal PII. For the purpose of this Agreement, the following terms mean:

1. "Assist in the Administration of the Medi-Cal Program" is performing an administrative function on behalf of Medi-Cal, such as determining eligibility or case managing IHSS (In-Home Supportive Services) clients; and

2. "Medi-Cal PII" is information directly obtained in the course of performing an administrative function on behalf of Medi-Cal, such as determining Medi-Cal eligibility or conducting IHSS operations, that can be used alone, or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, such as name, social security number, date of birth, driver's license number or identification number. PII may be electronic or paper.

AGREEMENTS

NOW THEREFORE, DHCS and the County Department mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. County Department workers covered by this Agreement ("County Workers") may use or disclose Medi-Cal PII only to perform functions, activities or services directly related to the administration of the Medi-Cal program in accordance with Welfare and Institutions Code section 14100.2 and 42 Code of Federal Regulations section 431.300 et.seq, or as required by law. For example, County Workers performing eligibility determinations may generally only use or disclose Medi-Cal PII to determine eligibility for individuals applying for Medi-Cal. County Workers assisting

in the administration of the In-Home Supportive Services (IHSS) program may generally use or disclose Medi-Cal PII only to perform administrative functions essential to the operation of the IHSS program. Disclosures which are required by law, such as a court order, or which are made with the explicit written authorization of the Medi-Cal client, are allowable. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of DHCS. No County Worker shall duplicate, disseminate, or disclose Medi-Cal PII except as allowed in this Agreement.

B. Access to Medi-Cal PII shall be restricted to only County Workers who need the Medi-Cal PII to perform their official duties in connection with the administration of the Medi-Cal program.

C. County Workers who access, disclose or use Medi-Cal PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. EMPLOYEE TRAINING AND DISCIPLINE

The County Department agrees to advise County Workers who have access to Medi-Cal PII of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the County Department shall:

A. Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII; and take corrective action against such County Workers who intentionally violate any provisions of this Agreement, up to and including by termination of employment. In complying with this requirement, the County Department agrees to:

1. Provide privacy and security awareness training to each new County Worker within 30 days of employment and thereafter provide ongoing reminders of the privacy and security safeguards in this Agreement to all County Workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII.

2. Maintain records indicating each County Worker's name and the date on which the initial privacy and security awareness training was completed.

3. Retain training records for inspection for a period of three years after completion of the training.

III. MANAGEMENT OVERSIGHT AND MONITORING

The County Department agrees to:

A. Establish and maintain ongoing management oversight and quality assurance for monitoring workforce compliance with the privacy and security safeguards in this Agreement when using or disclosing Medi-Cal PII.

B. Ensure that ongoing management oversight includes periodic self-assessments and randomly sampling work activity by County Workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII. DHCS shall provide the County Department with information on MEDS usage indicating any anomalies for investigation and follow-up.

C. Ensure that these management oversight and monitoring activities are performed by County Workers whose job functions are separate from those who use or disclose Medi-Cal PII as part of their routine duties.

IV. CONFIDENTIALITY STATEMENT

The County Department agrees to ensure that all County Workers who assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII sign a confidentiality statement. The statement shall include at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by the County Worker prior to access to Medi-Cal PII.

V. PHYSICAL SECURITY

The County Department shall ensure that Medi-Cal PII is used and stored in an area that is physically safe from access by unauthorized persons during working hours and non-working hours. The County Department agrees to safeguard Medi-Cal PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

A. Secure all areas of County Department facilities where County Workers assist in the administration of the Medi-Cal program and use or disclose Medi-Cal PII. The County Department shall ensure that these secure areas are only accessed by authorized individuals with properly coded key cards, authorized door keys or access authorization; and access to premises is by official identification.

B. Ensure that there are security guards or a monitored alarm system with or without security cameras 24 hours a day, 7 days a week at County Department facilities and leased facilities where a large volume of Medi-Cal PII is stored.

C. Issue County Workers who assist in the administration of the Medi-Cal program identification badges and require County Workers to wear these badges at County Department facilities where Medi-Cal PII is stored or used.

D. Store paper records with Medi-Cal PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks or locked offices in facilities which are multi-use, meaning that there are County Department and non-County Department functions in one building in work areas that are not securely segregated from each other. The County Department shall have policies which indicate that County Workers are not to leave records with Medi-Cal PII unattended at any time in vehicles or airplanes and not to check such records in baggage on commercial airplanes.

E. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing Medi-Cal PII.

VI. COMPUTER SECURITY SAFEGUARDS

The County Department agrees to comply with the general computer security safeguards, system security controls, and audit controls in this section.

General Computer Security Safeguards

In order to comply with the following general computer security safeguards, the County Department agrees to:

A. Encrypt portable computer devices, such as laptops and notebook computers that process and/or store Medi-Cal PII, with a solution using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution. One source of recommended solutions is specified on the California Strategic Sourced Initiative (CSSI) located at the following link: www.pd.dgs.ca.gov/masters/EncryptionSoftware.html. The County Department shall use an encryption solution that is full-disk unless otherwise approved by DHCS.

B. Encrypt workstations where Medi-Cal PII is stored using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified on the CSSI.

C. Ensure that only the minimum necessary amount of Medi-Cal PII is downloaded to a laptop or hard drive when absolutely necessary for current business purposes.

D. Encrypt all electronic files that contain Medi-Cal PII when the file is stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, etc.) using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified on the CSSI.

E. Ensure that all emails sent outside the County Department's e-mail environment that include Medi-Cal PII are sent via an encrypted method using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified on the CSSI.

F. Ensure that all workstations, laptops and other systems that process and/or store Medi-Cal PII have a commercial third-party anti-virus software solution and are updated when a new anti-virus definition/software release is available.

G. Ensure that all workstations, laptops and other systems that process and/or store Medi-Cal PII have current security patches applied and up-to-date.

H. Ensure that all Medi-Cal PII is wiped from systems when the data is no longer legally required. The County Department shall ensure that the wipe method conforms to Department of Defense standards for data destruction.

I. Ensure that any remote access to Medi-Cal PII is established over an encrypted session protocol using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified on the CSSI. The County Department shall ensure that all remote access is limited to minimum necessary and least privilege principles.

System Security Controls

In order to comply with the following system security controls, the County Department agrees to:

J. Ensure that all County Department systems containing Medi-Cal PII provide an automatic timeout after no more than 20 minutes of inactivity.

K. Ensure that all County Department systems containing Medi-Cal PII display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User shall be directed to log off the system if they do not agree with these requirements.

L. Ensure that all County Department systems containing Medi-Cal PII log successes and failures of user authentication and authorizations granted. The system shall log all data changes and system accesses conducted by all users (including all levels of users, system administrators, developers, and auditors). The system shall have the capability to record data access for specified users when requested by authorized management personnel. A log of all system changes shall be maintained and be available for review by authorized management personnel.

M. Ensure that all County Department systems containing Medi-Cal PII use role based access controls for all user authentication, enforcing the principle of least privilege.

N. Ensure that all County Department data transmissions over networks outside of the County's control are encrypted end-to-end using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified on the CSSI, when transmitting Medi-Cal PII. The County Department shall encrypt Medi-Cal PII at the minimum of 128 bit AES or 3DES (Triple DES) if AES is unavailable.

O. Ensure that all County Department systems that are accessible via the Internet or store Medi-Cal PII actively use either a comprehensive third-party real-time host based intrusion detection and prevention program or be protected at the perimeter by a network based IDS/IPS solution.

Audit Controls

In order to comply with the following audit controls, the County Department agrees to:

P. Ensure that all County Department systems processing and/or storing Medi-Cal PII have at least an annual system security review. The County Department review shall include administrative and technical vulnerability assessments.

Q. Ensure that all County Department systems processing and/or storing Medi-Cal PII have an automated audit trail, which includes the initiator of the request, along with a time and date stamp for each access. These logs shall be read-only and maintained for a period of at least three (3) years. There shall be a routine procedure in place to review system logs for unauthorized access. The County Department shall investigate anomalies identified by interviewing County Workers and witnesses and taking corrective action, including by disciplining County Workers, when necessary.

R. Maintain an automated audit trail record identifying either the individual worker or the system process that initiated a request for information from the Social Security Administration (SSA) for its systems, such as IEVS. Individual audit trail records shall contain the data needed to associate each query transaction to its initiator and relevant business purpose (that is, the client record for which SSA data was accessed) and each transaction shall be time and date stamped. Access to the audit file shall be restricted to authorized users with a need to know and the audit file data shall be unalterable (read only) and maintained for a minimum of three years.

S. Investigate anomalies in MEDS usage identified by DHCS and report conclusions of such investigations and remediation to DHCS.

T. Exercise management control and oversight, in conjunction with DHCS, of the function of authorizing individual user access to SSA data and MEDS and over the process of issuing and maintaining access control numbers and passwords.

U. Ensure that all County Department systems processing and/or storing Medi-Cal PII have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of data.

VII. PAPER DOCUMENT CONTROLS

In order to comply with the following paper document controls, the County Department agrees to:

A. Dispose of Medi-Cal PII in paper form through confidential means, such as cross cut shredding and pulverizing.

B. Not remove Medi-Cal PII from the premises of the County Department except for identified routine business purposes or with express written permission of DHCS.

C. Not leave faxes containing Medi-Cal PII unattended and keep fax machines in secure areas. The County Department shall ensure that faxes contain a confidentiality statement notifying persons receiving faxes in error to destroy them. County Workers shall verify fax numbers with the intended recipient before sending.

D. Use a secure, bonded courier with signature of receipt when sending large volumes of Medi-Cal PII. The County Department shall ensure that disks and other transportable media sent through the mail are encrypted using a vendor product that is recognized as an industry leader in meeting the needs for the intended solution, such as products specified on the CSSI.

VIII. NOTIFICATION AND INVESTIGATION OF BREACHES

The County Department agrees to:

A. Notify DHCS immediately by telephone call or e-mail upon the discovery of a breach of security of Medi-Cal PII in computerized form if the PII was, or is reasonably believed to have been, acquired by an unauthorized person; or within 24 hours by telephone call or e-mail of discovery of any other suspected security incident, intrusion, loss or unauthorized use or disclosure of PII in violation of this Agreement or the law. The County Department shall submit the notification to 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 PII, the County Department shall notify DHCS by calling the DHCS ITSD Help Desk.

DHCS Privacy Officer	DHCS Information Security Officer
Privacy Officer c/o: Office of Legal Services Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Help Desk (916) 440-7000 (800) 579-0874

B. Ensure that the initial notification includes contact and component information; a description of the breach or loss with scope, numbers of files or records, type of equipment or media, approximate time and location of breach or loss; description of how the data was physically stored, contained, or packaged (e.g. password protected, encrypted, locked briefcase, etc.); whether any individuals or external organizations have been contacted; and whether any other reports have been filed.

C. Take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment.

D. Investigate the breach and produce a written breach report within ten working days of the incident, detailing what data elements were involved; a description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PII; a description of where PII is believed to have been improperly transmitted, sent, or used; a description of the probable causes of the breach; a detailed corrective action plan including measures that were taken to halt and/or contain the breach. The County Department shall submit the breach report to the DHCS Privacy Officer and Information Security Officer.

E. Notify individuals of the breach or unauthorized use or disclosure of Medi-Cal PII maintained by the County Department when notification is required under state or federal law. The County Department shall obtain the approval of the DHCS Privacy Officer for the time, manner, and content of any such required notifications. County Department shall be responsible for the cost of such notification to the extent that such breach or unauthorized use or disclosure is due to the negligence or intentional misconduct of County Department. To the extent such breach or unauthorized use or disclosure is due to the negligence or intentional misconduct of DHCS, DHCS shall be responsible for notifying individuals and the County Department shall not be responsible for any costs of notification. If there is any question as to whether DHCS or the County Department is responsible for the breach, DHCS shall issue the notice and DHCS and the County Department shall subsequently determine responsibility for purposes of allocating the costs of such notices.

IX. COMPLIANCE WITH SSA AGREEMENT

The County Department agrees to comply with substantive privacy and security requirements in the Agreement between the Social Security Administration and DHCS, known as the 1137 Agreement, which is appended to and hereby incorporated into this Agreement (Exhibit A). The specific sections of the 1137 Agreement which contain substantive privacy and security requirements which are to be complied with by County Department are as follows: XI. Procedures for Security; XII. Safeguarding and Reporting Responsibilities for Personally Identifiable Information (PII); XIII. Procedures for Records Usage, Duplication, and Redisclosure Restrictions; and Attachment C, Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration. If there is any conflict between a privacy and security standard in these sections of the 1137 Agreement and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means that standard which provides the greatest protection to data.

X. COMPLIANCE BY COUNTY DEPARTMENT AGENTS

The County Department shall require that any agents, including subcontractors, which assist the County Department in its Medi-Cal functions and to which the County

Department provides PII, agree to the same privacy and security safeguards as are contained in this Agreement; and to incorporate, when applicable, the relevant provisions of this Agreement into each subcontract or sub-award to such agents or subcontractors.

XI. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions, the County Department agrees to allow DHCS to inspect the facilities, systems, books and records of the County Department, with reasonable notice from DHCS, in order to perform assessments and reviews. Such inspections shall be scheduled at times that take into account the operational and staffing demands of the county. The County Department agrees to promptly remedy any violation of any provision of this Agreement and certify the same to the DHCS Privacy Officer and Information Security Officer in writing, or to enter into a written corrective action plan with DHCS containing deadlines for achieving compliance with specific provisions of this Agreement.

XII. DEADLINE FOR SUBSTANTIAL COMPLIANCE

A. The County Department shall be in substantial compliance with this Agreement by no later than July 1, 2010.

B. If, at any time, the county is unable to meet the security and privacy requirements imposed in this Agreement in the manner specified therein due to a lack of funding; DHCS will work with the county to develop a Corrective Action Plan which can be implemented within the resources provided by the state for this purpose and which is intended to substantially meet those security and privacy requirements even if such requirements are met utilizing alternative or different methods than those specified in this Agreement.

C. DHCS shall monitor corrective action plans which County Department develops to remediate gaps in security compliance under this Agreement and reassess compliance.

XIII. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

In the event of litigation or administrative proceedings involving DHCS based upon claimed violations by the County Department of the privacy or security of Medi-Cal PII, or federal or state laws or agreements concerning privacy or security of Medi-Cal PII, the County Department shall make all reasonable effort to make itself and any subcontractors, agents, and County Workers assisting in the administration of the Medi-Cal program and using or disclosing Medi-Cal PII available to DHCS at no cost to DHCS to testify as witnesses. DHCS shall also make all reasonable efforts to make itself and any subcontractors, agents, and employees available to County Department at no cost to County Department to testify as witnesses, in the event of litigation or administrative proceedings involving the County Department based upon claimed violations by DHCS of the privacy or security of Medi-Cal PII, or state or federal laws or agreements concerning privacy or security of Medi-Cal PII.

XIV. SIGNATORIES

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.

The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement effective this _____ day of _____, 2008.

For the County of Humboldt, Department of Health and Human Services:

_____

Beverly Morgan Lewis
Director, County of Humboldt,
Department of Health and Human Services Social Services Branch

For the California Department of Health Care Services:

_____

Stan Rosenstein
Chief Deputy Director
Health Care Programs

Exhibit A: Agreement between the Social Security Administration and the State of California, Department of Health Care Services with Attachment "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration".

AGREEMENT BETWEEN THE SOCIAL SECURITY ADMINISTRATION AND THE STATE OF CALIFORNIA, DEPARTMENT OF HEALTH SERVICES (DEPARTMENT OF HEALTH CARE SERVICES)

TABLE OF CONTENTS

I. Purpose, Parties and Relationships, and Definitions 2
II. Legal Authority 6
III. Transfer of Data 8
IV. Justification and Anticipated Results 9
V. Systems Operations 10
VI. Description of the Records to be Matched 11
VII. Duration and Modification of the Agreement 113
VIII. Procedures for Notice 14
IX. Verification and Opportunity to Contest Match Data 14
X. Procedures for Retention and Timely Destruction of Identifiable Records 15
XI. Procedures for Security 16
XII. Safeguarding and Reporting Responsibilities for Personally Identifiable Information (PII) 17
XIII. Procedures for Records Usage, Duplication, and Redisclosure Restrictions 19
XIV. Accuracy Assessments 22
XV. Access by the Comptroller General 22
XVI. Additional Functions to be Performed under this Agreement 22
XVII. Reimbursement 223
XVIII. Persons to Contact 24
XIX. Authorized Officials 26
XX. Agency Approval 27
XXI. Signatures 28

I. Purpose, Parties and Relationships, and Definitions

A. Purpose (5 U.S.C. § 552a(o)(1)(A))

1. The purpose of this agreement is to establish terms, conditions and safeguards under which the Social Security Administration (SSA) agrees to disclose information relating to the eligibility for, and payment of, Social Security benefits and/or Supplemental Security Income (SSI) and Special Veterans Benefits (SVB), including certain tax return information as authorized by 26 U.S.C. § 6103, to the California Department of Health Services; to be succeeded with respect to all functions in this agreement by the California Department of Health Care Services as of July 1, 2007, hereinafter referred to as the State Agency, for use in:
   a. Verifying income and eligibility factors for State-administered programs authorized by sections 453 and 1137 of the Social Security Act (the Act) (see Article II.E.1.);
   b. Verifying Social Security numbers (SSNs) of applicants for, and recipients of, benefits under such programs; and
   c. Defining safeguards against unauthorized use and redisclosure of such information by the State Agency.

   This agreement also establishes the terms, conditions and safeguards under which SSA may disclose information relating to the eligibility for, and payment of, Social Security benefits and/or SSI and SVB, to the State Agency for use in State-administered program(s) that are a federal or federally funded program **not** authorized by sections 453 and 1137 of the Act, or that are programs not involving a federal or federally-funded benefit program; and that have been deemed compatible with SSA programs under SSA's regulations (see Article II.E.2.).

   Disclosure of tax return information to the State Agency for these programs is strictly prohibited unless explicitly authorized by 26 U.S.C. § 6103, and such authorization is clearly identified in Article II.E.2. of this agreement.

   This disclosure of information will ensure that the State Agency program(s) listed in Article II.E. has accurate information upon which to base its entitlement decisions.

   This computer matching agreement is executed under the Privacy Act of 1974, 5 U.S.C. § 552a, as amended by the Computer Matching and Privacy Protection Act of 1988 (CMPPA), as amended, and the regulations and guidance promulgated thereunder. While certain programs in Article II.E.2. may not constitute a matching program as defined by the Privacy Act, 5 U.S.C. § 552a(a)(8), the agencies agree to follow the applicable requirements of the CMPPA and other relevant provisions of the Privacy Act, 5 U.S.C § 552a.

2. Under the provisions of this agreement, a State Agency program is limited to the Data System(s) shown for that agency in Articles II.E.1. or II.E.2. of this agreement.

B. Agreement Parties and Relationships

The SSA component responsible for this matching agreement is the Office of Income Security Programs. The State Agency component responsible for this matching agreement is Department of Health Care Services. This agreement 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 agreement. This agreement will take precedence over any other documents that may be in conflict with it.

C. Definitions

1. "Agent" see "Contractor/Agent"

2. "BENDEX" means the Beneficiary and Earnings Data Exchange System.

3. "Contractor/Agent" means a third-party entity in a contractual or similar relationship with the State Agency to act on the Agency's behalf to administer, or assist in administering, an income-maintenance or health-maintenance program described in this agreement.

4. "Cost-benefit data" means the measure of the match effectiveness. The Computer Matching and Privacy Protection Act (CMPPA) of 1988, Pub. L. 100-503, requires a cost-benefit analysis as part of an agency decision to conduct or participate in a matching program.

5. "DIB" means the Data Integrity Board.

6. "Equivalent Information" means the earnings amounts from employment not covered under the Act converted to information equivalent to quarters of coverage information provided for work covered by the Act.

7. "EVS" means the Enumeration Verification System. Prior to the development of the SVES, SSA provided electronic SSN verification via EVS. The EVS still exists and is currently used by SSA and some states.

8. "Food Stamp" means, for purposes of the quarters of coverage aspect of this matching program as authorized under the above-cited provisions of Pub. L. 104-193, the program defined in
7 U.S.C. § 2012(h) of the Food Stamp Act of 1977.

9. "FISMA" means the Federal Information Security Management Act (http://csrc.nist.gov/sec-cert/).

10. "FTMS" means the SSA File Transfer Management System.

11. "Health Maintenance Program" (if appropriate) means a noncommercial program designed to provide an individual with health care (both preventive and treatment) or to subsidize the cost of such care (e.g., Medicare, Medicaid). Note: A commercial insurance company, acting as a contractor/agent of the State Agency, may administer such a program for a State or local agency.

12. "Income Maintenance Program" (if appropriate) means a noncommercial program designed to provide an individual with basic necessities of life (e.g., food, clothing, shelter, utilities) or to supplement the individual's income to permit the purchase of such necessities (e.g., subsidized housing, Food Stamp, Temporary Assistance for Needy Families (TANF), general assistance, Title XX services, energy assistance, State supplementation).

13. "IRC" means the Internal Revenue Code.

14. "MBR" means the Master Beneficiary Record.

15. "MEF" means the Master Earnings File, also known as the Earnings Recording and Self-Employment Income System.

16. "MULTX" means the relationship between multiple SSNs associated with an individual.

17. "NUMIDENT" means a subsystem of the Master Files of SSN Holders and SSN Applications.

18. "OMB" means the Office of Management and Budget.

19. "PII" means Personally Identifiable Information. PII is the information obtained from SSA that can be used, alone or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files. Examples of PII may include: name, SSN, Social Security benefit data, date of birth, official State or government issued driver's license or identification number.

20. "PUPS" means the Prisoner Update Processing System.

21. "Quarters of Coverage" means quarters of coverage as assigned and described under Title II of the Act. The term "quarters of coverage" is also referred to as "credits" in various SSA public information documents. The term "Social

Security credits" may be used interchangeably as well. Quarters of coverage as used in this agreement may also refer to "qualifying quarters" which would entitle individuals to receive Food Stamps.

22. "SDX" means the State Data Exchange.

23. "SSA" means the Social Security Administration.

24. "SSI" means the Supplemental Security Income program established under Title XVI of the Social Security Act.

25. "SSN" means Social Security number.

26. "SSR/SVB" means the Supplemental Security Income Record and Special Veterans Benefits.

27. "State Administered Program" means any means-tested public benefits program of a State or political subdivision of a State under which the State or political subdivision specifies the standards for eligibility.

28. "State Agency" means the agency defined in Article I.A. above, the California Department of Health Care Services, including any applicable county, local, or other office thereof, regardless of whether the employees of the agency are State, county, or local government employees.

29. "State Transmission/Transfer Component" or "STC" (Also known as "Computer Data Center") , if applicable based on Article III, means an entity that, under a separate agreement with SSA, has agreed to transfer data files between SSA and the State Agency identified in Article I.A.

30. "SVB" (if appropriate) means the Special Veterans Benefits established under Title VIII of the Act. Under this program, certain World War II veterans who were eligible for benefits under Title XVI when Title VIII was enacted on December 14, 1999, may be entitled to receive a special benefit for each month they subsequently reside outside the United States after April 2000.

31. "SVES" means the State Verification and Exchange System.

32. "Tax Return Information" has the same meaning as given in 26 U.S.C. § 6103(b). For purposes of this agreement, "tax return information" includes SSA's records obtained under the authority of 26 U.S.C. § 6103 and 42 U.S.C. § 432 concerning the amount of an individual's earnings from wages and/or self-employment income, the periods involved, the identities and addresses of employers, and the amount of payment of retirement income.

II. Legal Authority (5 U.S.C. § 552a(o)(1)(A))

This agreement sets forth the responsibilities of SSA and the State Agency with respect to information obtained pursuant to the agreement which is permitted by the Privacy Act of 1974, as amended and SSA's Privacy Act Regulations (20 C.F.R. § 401.150). The agreement takes into account SSA's responsibilities under section 1106 of the Act (42 U.S.C. § 1306) (see Attachment A) and the responsibilities of SSA and the State Agency under the Internal Revenue Code (IRC) (26 U.S.C. § 6103).

A. Program Data and Tax Return Data

This matching program is authorized for the State Agency programs listed in Article II.E.1. by law under sections 1137 and 453 of the Act (42 U.S.C. §§ 1320b-7 and 653). Section 1137 mandates that the States use an income and eligibility verification system to administer the federally-funded benefit programs (e.g., Medicaid, TANF, Food Stamp and Unemployment Compensation programs). This agreement implements this section by allowing SSA to disclose the data necessary for the State's administration of these programs. 26 U.S.C. § 6103(l)(7) only authorizes the disclosure of tax return information to State Agencies administering programs under section 1137 of the Act for the purpose of administering said programs. Section 453 of the Act authorizes SSA to disclose data to the State Child Support Enforcement Agencies and the States on the location, income and assets of child support obligors, to assist States in establishing paternity and establishing, setting the amount of, modifying, or enforcing child support obligations. For purposes of, and to the extent necessary in establishing and collecting child support obligations from, and locating individuals owing such obligations pursuant to an approved State IV-D plan, SSA is also authorized to disclose certain tax return information to State Agencies (26 U.S.C. § 6103(l)(8)). Contractors/agents acting on behalf of a State will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103.

B. Prisoner and Death Data

SSA may, under this agreement, disclose prisoner and death data to the State Agency for the administration of the federally-funded benefit programs. The authority for the disclosure of prisoner data is contained in section 202(x)(3)(B)(iv) of the Social Security Act (42 U.S.C. § 402 (x)(3)(B)(iv)). Section 205(r)(3) of the Social Security Act (42 U.S.C. § 405(r)(3)) is the authority for the disclosure of death data.

Under the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2), SSA provides death indicators for restricted State death data.

C. Quarters of Coverage Data

The quarters of coverage aspect is authorized by sections 402, 412, 421 and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, 1645). For purposes of implementation, which involves the significance of Social Security quarters of coverage to the eligibility of certain aliens for certain defined Federal and State public benefits, SSA may under this agreement disclose to the State Agency, to the extent permitted by law, quarters of coverage and equivalent information.

The Federal programs mandatorily or potentially affected by the above-referenced sections of Pub. L. 104-193 are: SSI, Food Stamp, and TANF under part A of Title IV of the Act; SVB under Title VIII of the Act; social services block grants under Title XX of the Act; and State Medicaid plans approved under Title XIX of the Act.

D. Compatible Programs and Data Disclosure

This matching program is also authorized for the programs listed in Article II.E.2. by the routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3). The Privacy Act permits SSA to authorize the disclosure of records for "routine uses" if the use of such records is compatible with the purpose for which the record was collected (5 U.S.C. § 552a(a)(7)). SSA has deemed certain other Federal and State programs compatible to SSA programs, similar to the nature of the programs set forth in section 1137 of the Act. SSA has also determined that the disclosure of records to certain agents acting on behalf of a Federal or State Agency that are assisting or administering a program compatible with SSA programs is permissible. SSA has determined that these other State programs currently meet the requirements for compatibility (20 C.F.R. § 401.150) in that the purposes for which the information will be disclosed are consistent with the purposes for which SSA originally collected the information (i.e., the information will be used in other programs that have the same purposes as SSA programs; the information concerns eligibility, benefit amounts, or other matters of benefit status in a Social Security program; and the information is relevant to determining the same matters in the other program). Disclosure of tax return information to a State Agency for these programs is strictly prohibited unless explicitly authorized by 26 U.S.C. § 6103 and such authorization is clearly identified in Article II.E.2. of this agreement.

E. Department of Health Care Services Program(s) Covered under this Agreement*

1. Programs authorized to receive SSA's SDX-BENDEX-SVES data (includes tax data) based on sections 1137 and 453 of the Act:

Program	Data System(s)	Description
Medicaid	SDX, BENDEX, EVES, SVES, and quarters of coverage	Administration of Medicaid

2. Other programs authorized by the routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3) to receive certain data (excludes tax data):

Program	Data System(s)	Description

*Any changes must be reported to SSA as they occur.

III. Transfer of Data *(prior to printing, place an "X" in the appropriate box)*

☐ Data will be transmitted directly between SSA and the **California Department of Health Care Services** by ***(indicate FTMS or (method of data transmission))***, a secure mechanism approved by SSA.

The **California Department of Health Care Services** will not transfer or disclose this data to any other agency or entity (e.g. State contractor) by any means without amending this agreement or entering into a new agreement which would allow for the data transfer.

☒ Data will be transmitted directly between SSA and the State of California, Department of Technology Services by Connect:Direct, a secure mechanism approved by SSA. The California Department of Technology Services, as a State Transmission/Transfer Component (STC), will serve as the conduit between SSA and the California Department of Health Care Services. The STC has a separate agreement with SSA defining what data SSA will disclose and the terms under which SSA will provide such data.

The California Department of Health Care Services will not transfer or disclose this data to any other agency or entity (e.g. State contractor) by any means without amending this agreement or entering into a new or amended agreement which would allow for the data transfer.

IV. Justification and Anticipated Results (5 U.S.C. § 552a(o)(1)(B))

A. Justification

1. The State Agency program(s) listed in Article II.E.1. are required to use information relating to eligibility for and amount of Social Security benefits and/or SSI and SVB benefits, quarters of coverage, prisoner, and death information under the Act, and, where appropriate, certain tax return information, for administration of the specific State programs covered by this agreement. Additional programs mandated by law after the inception of this agreement may, by the means of modification to Article II.E., be added to the coverage of this agreement.

2. SSA is required by law to disclose certain information to the State Agency and agrees to provide quarters of coverage information to the State for purposes of Pub. L. 104-193. Under Pub. L. 104-193, the State Agency may be required to determine the number of quarters of coverage of certain alien applicants and their parents and spouses in determining the eligibility of such applicants for certain defined public benefits. SSA at its discretion, to the extent permitted by law, may provide to the State Agency quarters of coverage information and equivalent information recorded in the applicant's account or the accounts of the parents or spouse of such applicant.

3. The State Agency is required by law to require each applicant for, or recipient of, benefits under the 1137 programs listed in Article II.E., to furnish his or her SSN or identifying information and to utilize such number or identifying information in the administration of the programs. SSA is required by law to verify the SSN of individuals applying for these State-administered benefit programs.

4. SSA is required by law to disclose data to the State Child Support Enforcement Agencies (CSEA) and the States on the location, income and assets of child support obligors, to assist States in establishing paternity and establishing, setting the amount of, modifying, or enforcing child support obligations. For purposes of, and to the extent necessary in establishing and collecting child support obligations from, and locating individuals owing such obligations pursuant to an approved State IV-D plan, SSA is authorized to disclose Social Security benefits and/or SSI and SVB benefits, quarters of coverage, prisoner, and death information under the Act, and certain tax return information, for administration of State child support enforcement programs. The Federal Parent Locator System (FPLS) was developed for this purpose and is the most efficient and preferred method of this data transfer.

5. The use of computer technology to transfer data from SSA to the State Agency is more efficient and quicker than the use of manual processes.

B. Anticipated Results

The State Agency expects program savings of $200,400,000 over the period of this agreement at a cost of $600,000 by performing this matching program. SSA does not expect any direct program savings to result from this matching program, but based on cost-benefit analysis, estimates SSA net administrative savings of approximately $21.8 million for all the SDX/BENDEX/SVES data exchanges through increased efficiencies in coordinating the administration of mutually dependent Federal and State programs. In such fashion, the matching program is expected generally to benefit federally-funded programs that are State administered.

V. Systems Operations

These matches are initiated in the following ways:

A. The SDX aspect of this matching program is operated by SSA periodically sending the State Agency a file of SSI and SVB recipients in that State who are currently receiving SSI and SVB payments, or were recently terminated, or had changes in status.

B. The BENDEX aspect of this matching program is operated by the State Agency periodically sending to SSA a file of applicants for, or recipients of, benefits under certain State-administered programs (see Article II.E.) for whom Social Security benefit information and/or earnings data is required.

C. The EVS aspect of this matching program is operated by the State Agency periodically sending to SSA a file of applicants for, or recipients of, benefits under certain State-administered programs (see Article II.E.) for whom SSN verification is required.

D. The SVES aspect of this matching program is operated by the State Agency periodically sending to SSA a file of applicants for, or recipients of, benefits under certain State-administered programs (see Article II.E.) for whom Social Security, SSI and SVB benefit information and/or SSN verification is required.

E. The quarters of coverage aspect of this matching program is operated by the State Agency periodically sending to SSA a file of applicants for, or recipients of, benefits under certain State-administered programs (see Article II.E.) and, where permitted by applicable law, the parents or spouses of such applicants when requesting quarters of coverage or equivalent information necessary for the implementation of the above-referenced sections of Pub. L. 104-193.

F. The prisoner aspect of this matching program is operated by the State Agency periodically sending to SSA a file of applicants for, or recipients of, benefits under certain State-administered programs (see Article II.E.) for the State Agency to verify

and otherwise ensure that benefits are not issued to individuals who are not entitled to receive such benefits.

VI. Description of the Records to be Matched (5 U.S.C. § 552a(o)(1)(C))

A. Systems of Records (see data elements at Attachment B)

1. SSA's systems of records used for purposes of this agreement may be the SSR/SVB, MBR, Earnings Recording and Self-Employment Income System (subsystem referred to as the MEF), Master Files of SSN Holders and SSN Applications (subsystems referred to as the EVS, the ALPHIDENT, or the NUMIDENT), and PUPS. MULTX, the systems program that associates multiple SSNs that are related to the applicant's earnings file, may also be used.

2. For each aspect of this matching program, the following are the SSA systems of records that will be accessed:
   a. SDX – SSR/SVB, SSA/ODSSIS (60-0103);
   b. BENDEX – MBR, SSA/ORSIS (60-0090) and the Earnings Recording and Self-Employment Income System, SSA/OEEAS (60-0059);
   c. EVS – Master Files of SSN Holders and SSN Applications, SSA/OEEAS (60-0058);
   d. SVES – SSR/SVB, SSA/ODSSIS (60-0103); MBR, SSA/ORSIS (60-0090); Earnings Recording and Self-Employment Income System, SSA/OEEAS (60-0059); Master Files of SSN Holders and SSN Applications, SSA/OEEAS (60-0058); and PUPS, SSA/OEEAS (60-0269);
   e. Quarters of Coverage Query – Earnings Recording and Self-Employment Income System, SSA/OEEAS (60-0059) and the Master Files of SSN Holders and SSN Applications, SSA/OEEAS (60-0058);
   f. Prisoner Query – PUPS, SSA/OEEAS (60-0269).

3. SSA and the State Agency will exchange information through FTMS or a mutually acceptable security mechanism.

B. Specified Data Systems Used in a Match

1. SDX – When the State Agency receives SSI and SVB program data and uses this data in matching activities, it will match the SDX file to the appropriate fields in State files.

2. BENDEX – The State Agency will provide SSA with name, SSN, and date of birth for those individuals about whom information is requested from BENDEX.

3. EVS – The State Agency will provide SSA with name, SSN, and date of birth for those individuals about whom SSN verification is requested from EVS.

4. SVES – The State Agency will provide SSA with name, SSN, and date of birth for those individuals about whom information is requested from SVES.

5. Quarters of Coverage Query – The State Agency will provide SSA with name, SSN, and date of birth for those individuals about whom information is requested from SVES.

6. Prisoner Query – The State Agency will provide SSA with name, SSN, and date of birth for those individuals about whom information is requested from PUPS.

C. Number of Records Involved

1. SDX – SSA will furnish to the State Agency daily SDX files containing information on SSI and SVB recipients. The number of records given to the State Agency during a month will be approximately 660,000.

2. BENDEX – The State Agency will furnish to SSA daily files containing identifying information of applicants for, or recipients of, benefits under State-administered programs. The State Agency will be requesting approximately 2,750,000 records each month from SSA.

3. EVS – The State Agency will furnish to SSA daily SSNs of applicants for, or recipients of, benefits under State-administered programs. The State Agency will be requesting approximately 1,100,000 records each month from SSA.

4. SVES – The State Agency will furnish to SSA daily files containing identifying information of applicants for, or recipients of, benefits under State-administered programs. The State Agency will be requesting approximately 1,760,000 records each month from SSA.

5. Quarters of Coverage Query – The State Agency will furnish to SSA monthly files containing identifying information of applicants for, or recipients of, benefits under State-administered programs. The State Agency will be requesting approximately 110,000 records each month from SSA.

6. Prisoner Query – The State Agency will furnish to SSA N/A files containing identifying information of applicants for, or recipients of, benefits under State-administered programs. The State Agency will be requesting approximately N/A records each month from SSA. Not being used by the Department of Health Care Services.

If the State Agency anticipates an unprecedented increase to the number of records shown above, the State Agency agrees to contact the SSA Systems contact (see Article XVIII.A.) prior to initiating that month's match(es).

VII. Duration and Modification of the Agreement

A. Duration

1. This agreement can only be effectuated and will only be available for use the later of:
   a. July 1, 2007, OR
   b. 40 days after submission of matching notices on this program to Congress and OMB, or 30 days after publication of the computer matching notice for this matching program in the Federal Register, and upon signature of the agreement by both parties to the agreement.

2. This agreement requires signoff by both agencies and will be effective upon the date of the SSA Regional Commissioner's signature. This agreement will be in effect for 18 months, but not beyond December 31, 2009. If at the end of 18 months December 31, 2009, is in the future, this agreement may be extended.

   The extension may be for up to 12 months, but not beyond December 31, 2009. In the extension, SSA's Data Integrity Board (DIB), and the State Agency will certify, within 3 months prior to the expiration of the agreement, pursuant to 5 U.S.C. § 552a(o)(2)(D) that:
   a. The matching program will be conducted without change; and
   b. The matching program has been conducted in compliance with the original agreement.

3. The provisions of this agreement may **not** extend beyond December 31, 2009.

4. If either agency does not wish to renew this agreement, it will notify the other of its intention not to renew at least 90 days before the end of the then current period.

5. Either party may unilaterally terminate the agreement upon written notice to the other party, in which case the termination will be effective 90 days after the date of the notice, or at a later date specified in the notice. The agreement may be terminated at any time by the mutual written consent of both parties. However, SSA may make an immediate, unilateral suspension of the data flow and/or termination of this agreement if SSA:
   a. Has determined that there has been an unauthorized use or disclosure of information by the State Agency and/or their contractors/agents; or

b. Has determined that there has been a violation of or failure to follow the terms of this agreement; or

c. Has reason to believe that the State Agency and/or their contractors/agents breached the terms for security of data until such time as SSA makes a definite determination of a breach.

6. This agreement does not authorize SSA to incur obligations through the performance of the services described herein. Since SSA's performance under this agreement spans multiple fiscal years, SSA's ability to perform work for each fiscal year is subject to the availability of funds.

B. Modification

This agreement may be modified at any time by an amendment or new agreement which satisfies both parties.

VIII. Procedures for Notice (5 U.S.C. § 552a(o)(1)(D))

A. Applicants

Both the State Agency and SSA agree to notify all individuals who apply for benefits for their respective programs that any information provided by them is subject to verification through matching programs. The State Agency's notice consists of appropriate language printed on application forms (DHS MC210 – mail in Medi-Cal application, SAWS 2 – Statement of Facts, MC321- joint Medi-Cal/Healthy Families application, MC368 - Important Information for Medi-Cal applicants, MC219 - Important Information For Persons Requesting Medi-Cal, -, and MC266 - Directions To Apply for Medi-Cal" (presumptive eligibility), and through separate handouts with federally approved language. SSA's notice consists of appropriate language printed on its application forms or a separate handout with appropriate language when necessary.

B. Beneficiaries/Annuitants

Both the State Agency and SSA will provide subsequent notices to their respective retirees, annuitants, beneficiaries, and/or recipients. The State Agency's notice consists of appropriate language printed on application forms (MC219 - Important Information For Persons Requesting Medi-Cal, and MC262 - Redetermination for Medi-Cal beneficiaries (Long-term care in own MFBU), and through separate handouts with federally approved language. SSA's notice consists of a notice of this matching program in the Federal Register and periodic mailings to all beneficiaries and recipients describing SSA's matching activities.

IX. Verification and Opportunity to Contest Match Data
(5 U.S.C. § 552a(o)(1)(E) and 5 U.S.C. § 552a(p))

A. Verification

Based on the determination of SSA's DIB pursuant to its approval of this agreement, unless contradictory OMB final guidelines are issued, the State Agency may consider all SSA benefit data disclosed under this agreement as verified, as provided in 5 U.S.C. § 552a(p)(1)(A)(ii). Thus, the DIB has determined that the information is limited to identification and amount of benefits paid by SSA under a Federal benefit program and there is a high degree of confidence in the accuracy of the data (see Article XIV. below). The State Agency may use the above-specified data without independent verification in their administration of the program(s) listed in Article II.E.

Prisoner and death data, however, do not have this high degree of accuracy; and before any adverse action can be taken against any individual, this data must be independently verified.

Tax return information obtained under this agreement, as authorized by 26 U.S.C. § 6103, will be verified in accordance with section 1137 of the Social Security Act.

B. Opportunity to Contest

The State Agency agrees that there can be no termination, suspension, reduction, final denial, or other adverse action taken against an individual based on this computer match with SSA until there is an opportunity to contest the match information such that:

1. Notice is provided by the State Agency to the affected individual which informs that individual of the match findings and the opportunity to contest these findings.

2. The affected individual is given until the expiration of any time period established for the relevant benefit 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.

3. The notice clearly states that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the match data provided by SSA is correct and will make the necessary adjustment to the individual's payment.

X. Procedures for Retention and Timely Destruction of Identifiable Records (5 U.S.C. § 552a(o)(1)(F))

A. State Agency

The State Agency and programs listed in Article II.E. will retain all identifiable records received from SSA only for the period of time required for any processing related to the matching program and will then destroy the records.

As part of the matching program, any accretions, deletions, or changes to SSA's program rolls provided by SSA to the State Agency can be used by the State Agency to update its master files, which will be permanently retained under cognizable authority governing the State Agency's retention of records. Any other identifiable records must be destroyed unless the information has to be retained in individual file folders in order to meet evidentiary requirements. In the latter instance, the State Agency will retire identifiable records in accordance with the Department of Health Care Services Manual of Policies and Procedures, Division 23-353 (Retention Period) and 23-355 (Destruction of Case Records), consistent with the requirements of the Privacy Act (5 U.S.C. 552a]0]).

B. SSA

SSA will delete electronic data input files received from the State Agency when the match has been completed. SSA will retire identifiable records in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

C. Neither SSA nor the State Agency will create a separate file or system concerning only individuals whose records are used in this matching program.

XI. Procedures for Security (5 U.S.C. § 552a(o)(1)(G))

A. At a minimum, SSA will safeguard the State Agency's information and the State Agency will safeguard SSA's information as follows:

1. Access to the records matched and to any records created by the match will be restricted to only those authorized employees and officials who need it to perform their official duties in connection with the uses of the information authorized in this agreement.

2. The records matched and any records created by the match will be stored in an area that is physically safe from access by unauthorized persons during duty hours, as well as non-duty hours, or when not in use.

3. The records matched and any records created by the match will be processed under the immediate supervision and control of authorized personnel in a manner which will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve any such records by means of computer, remote terminal, or other means.

4. All personnel who will have access to the records matched and to any records created by the match will be advised of the confidential nature of the information, the safeguards required to protect the information, and the civil and criminal sanctions for noncompliance contained in applicable Federal laws.

5. The equipment, files and/or documents will be transported under appropriate safeguards.

B. The Secretary of the Treasury has published a brochure entitled "Tax Information Security Guidelines for Federal, State and Local Agencies," Publication 1075, which is available from the Internal Revenue Service (IRS) District Disclosure Officer in the appropriate IRS district. SSA and the State Agency agree to comply with these guidelines and any revision of them, submit to IRS audits, and furnish the required reports to IRS. The aforementioned brochure is hereby incorporated by reference into this agreement.

SSA's Office of Systems Security Operations Management has prepared written guidelines entitled, "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration." These guidelines (see Attachment C) provide instructions and an explanation of SSA's security requirements. Additional copies are available upon request. By signing this agreement, the State Agency agrees to comply with SSA's security guidelines.

C. Both SSA and State Agency agree to comply with the requirements of the Federal Information Security Management Act (FISMA) (Pub. L. 107-347, Title III, section 301) as it applies to the electronic storage, transport of records between agencies, and the internal processing of records received by either Agency under terms of this agreement. SSA reserves the right to conduct onsite inspections to monitor compliance with FISMA regulations during the lifetime of this agreement.

D. Both SSA and State Agency agree to inform personnel including contractors/agents of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.

E. SSA recognizes States already are subject to IRS safeguard reviews which require States to meet a high degree of compliance; and as a result, SSA's future review activity will complement, rather than duplicate, IRS security requirements and review activity.

XII. Safeguarding and Reporting Responsibilities for Personally Identifiable Information (PII)

A. State Agency

1. The State Agency will ensure that its employees and contractors/agents properly safeguard PII furnished by SSA under this agreement from loss, theft or inadvertent disclosure.

2. The State Agency will ensure that its employees and contractors/agents understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee or the contractor/agent is at his or her regular duty station.

3. The State Agency will ensure that laptops and other electronic devices/media containing PII and used by its employee and its contractors/agents are encrypted and/or password protected.

4. The State Agency will ensure that when it and/or its contractors/agents are sending email containing PII, its employees and/or contractors/agents do so only from and to addresses that are secure or that they have encrypted the email.

5. The State Agency will ensure that its employees and its contractors/agents working under this agreement adhere to the procedures listed in this agreement.

6. The State Agency will ensure that its employees or contractors/agents limit disclosure of the information and details relating to a PII loss only to those with a need to know.

7. The State Agency will establish procedures to ensure that when a State Agency employee or contractor/agent becomes aware of the possible or suspected loss of PII, the State Agency Systems Security Issues contact or equivalent is immediately notified of the incident. The State Agency will then notify the SSA Regional Office contact (see Article XVIII.A.3.). If within 1 hour the State Agency has been unable to speak with the SSA Regional Office contact or if for some other reason, e.g., it is outside of the Regional Office's normal business hours, the State Agency will call SSA's Network Customer Service Center (NCSC) at 410-965-7777 or toll free at 1-888-772-6111.

   When reporting the loss or suspected loss of PII, the report should include the following specific information:

   a. Contact and component information.
   b. A description of the loss or suspected loss (e.g., nature of loss, scope, number of files or records and type of equipment or media) including the approximate time and location of the loss.
   c. How was the data physically stored, packaged and/or contained (e.g., password protected, encrypted, locked briefcase, redacted personal information, etc.)?
   d. Which SSA and/or State components and/or state contractor/agents have been involved?
   e. Have any individuals or external organizations (e.g., other agencies, law enforcement or the press) been contacted or contacted you?

f. Have any other reports (e.g., local police, SSA and/or State reports) been filed?
g. Any other pertinent information.

8. The State Agency will provide updates as they become available to the SSA Systems Security Issues contact, as applicable. The State Agency will provide complete and accurate information about the details of the possible PII loss to assist the SSA Systems Security Issues contact. The State Agency and/or contractor/agent will use the worksheet (see Attachment D) to quickly gather and organize information about the incident.

B. SSA

1. SSA will assume responsibility for making the contact within SSA so that a formal report is filed in accordance with SSA procedures.

2. SSA will notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of personally identifiable information related to a data exchange covered under this agreement occurs.

XIII. Procedures for Records Usage, Duplication, and Redisclosure Restrictions (5 U.S.C. § 552a(o)(1)(H) and 5 U.S.C. § 552a(o)(1)(I))

A. The State Agency agrees to the following limitations on the use, duplication, and redisclosure of the data systems listed in Article VI.B. and information provided by SSA:

1. The tax return information the BENDEX contains will be used only to determine individual eligibility for, or the amount of, assistance under a State plan pursuant to section 1137 of the Act. Contractors/Agents acting on behalf of a State will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103. The other data provided by SSA will not be redisclosed or used for any purpose other than to determine eligibility for, or the amount of, benefits under the State-administered income/health maintenance programs specified in Article II.E. Such State-administered programs must be authorized in statements of routine use published by SSA in the Federal Register or otherwise specifically approved by SSA and not otherwise prohibited by applicable law.

2. The tax return information the BENDEX contains and the other data provided by SSA will not be used to extract for any purpose information concerning individuals who are neither applicants for, nor recipients of, benefits under the State-administered income/health maintenance programs specified in Article II.E. Information will be used in a manner provided for by applicable law and described in this agreement. Disclosures to such State-administered programs must be authorized in statements of routine use published by SSA in the

Federal Register or otherwise specifically approved by SSA and not otherwise prohibited by applicable law.

3. The State Agency will restrict access to the information obtained from SSA to only those authorized State employees and contractors/agents under contract with the State Agency who need it to perform their official duties in connection with the intended uses of the information authorized in this agreement. At SSA's request, the State Agency will obtain from its contractor/agent a current list of the contractor's/agent's employees who have access to SSA information under the terms of this agreement.

4. Except as necessary for the operation of this matching program, as provided in this agreement, files provided by SSA will not be duplicated or disseminated within or outside the State Agency without the prior written approval of SSA. SSA will not grant such authority unless the redisclosure is required by law or is essential to the matching program. In such instances, the State Agency must specify in writing what records are being disclosed, to whom, and the reasons that justify such redisclosure.

5. Except as necessary for the operation of this match, as provided for in this agreement, State Agency contractors/agents and their employees who are authorized access to the information provided under this agreement will not duplicate, disseminate or disclose the SSA files provided to them by the State Agency unless the State Agency has obtained SSA's prior written approval for redisclosure.

6. The State Agency will undertake in its contractual relationship with each contractor/agent to obtain the contractor's written agreement that the contractor/agent will abide by all relevant Federal laws and access, disclosure and use restrictions, and security requirements in this agreement. The State Agency will provide the contractor/agent with a copy of this agreement and the related attachments before the initial disclosure of data to the contractor/agent.

7. Prior to signing this agreement the State Agency agrees to provide to SSA's Regional Office contact(s) (see Article XVIII.A.) written communication on State Agency letterhead:
   a. that the State Agency is not using contractors/agents; or
   b. a current list of contractors/agents who, as of the effective date of this agreement, will have access to the information the State Agency obtains through this agreement. The list will contain: name and address of contracting firm, description of the work that is performed with the information and the location of where work is performed with the information. The State Agency further agrees to certify, in this same manner, to SSA that these contractors/agents are currently under contract with the State Agency and are acting on behalf of the State Agency to administer or assist in administering the programs listed in Article II.E.

8. For the duration of this agreement and within 60 days of an occurrence, the State Agency agrees to provide to SSA Regional Office contact (see Article XVIII.A.3.) written communication on State Agency letterhead whenever a new contractor/agent will have access to information under this agreement, or an existing contractor/agent will no longer have access to the information under this agreement.

9. Prior to the renewal of this agreement, the State Agency agrees to provide to SSA Regional Office contact(s) (see Article XVIII.A.) written communication on State Agency letterhead certification that all contractors/agents administering or assisting in administering the programs listed in Article II.E are in compliance with this agreement.

10. State Agency employees and contractors/agents under contract with the State Agency who access, disclose or use the information obtained pursuant to this agreement in a manner or for a purpose not authorized by the agreement may be subject to civil and criminal sanctions contained in applicable federal statutes.

11. SSA files provided to the State Agency remain the property of SSA and will be handled as provided in Article X.A., once matching activity under this agreement is complete.

B. SSA agrees to the following limitations on the use, duplication, and redisclosure of the identifying files and information provided by the State Agency (see Article VII.B):

1. The files provided by the State Agency will be used and accessed only for the purposes specified in this agreement.

2. The files provided by the State Agency will not be used to extract information concerning the individuals therein for any purpose not specified in this agreement.

3. The files provided by the State Agency will not be duplicated or disseminated within or outside SSA without the written permission of the State Agency.

4. The files provided by the State Agency remain the property of the State Agency and will be handled as provided in Article X.B., once matching activity under this agreement is completed.

C. Both SSA and the State Agency will adopt policies and procedures to ensure that information contained in their respective records and obtained from each other will be used solely as provided in this agreement, including adherence to the terms of section 1106 of the Social Security Act

(42 U.S.C. § 1306), section 6103(p)(4) of Title 26 of the IRC for tax return information, and the regulations promulgated thereunder.

XIV. Accuracy Assessments

Previous matches with the same files indicate that the State Agency's records are 97 % accurate based on inputs from recipients and third parties, and that SSA's benefit records are more than 99% accurate when they are created. The prisoner and death records, some of which are not verified by SSA, do not have this high degree of accuracy.

XV. Access by the Comptroller General (5 U.S.C. § 552a(o)(l)(K))

The Government Accountability Office (Comptroller General) may have access to State Agency and SSA records that the Comptroller General deems necessary in order to monitor or verify compliance with this agreement.

XVI. Additional Functions to be Performed under this Agreement

A. The State Agency agrees:

1. The SDX, BENDEX, and SVES systems will be used by the State Agency to obtain Social Security, SSI and SVB payment information on the applicants/recipients of the programs identified in Article II.E. The State Agency also agrees that it will use BENDEX and/or SVES to obtain tax return information and/or quarters of coverage, prisoner, and death information pertaining to only those persons for which use is authorized by applicable law pursuant to section 1137 of the Social Security Act, as specified in this agreement. Use and disclosure of this information for other purposes are subject to the restrictions described in this agreement.

2. To provide information obtained in the quarters of coverage query, as necessary, to State and local government agencies within the State which will make quarters of coverage determinations under Pub. L. 104-193.

3. To provide SSA with the necessary identifying information concerning those individuals about whom information is requested from BENDEX or SVES. (Specific requirements for the request are discussed in the BENDEX handbook or SVES manual.) The State Agency also agrees to notify SSA when an individual is no longer eligible for benefits.

4. To submit SSNs for verification through EVS or SVES in the format specified by SSA. If SSA notifies the State Agency that the SSN and identifying information do not match, the client should be asked about other names used and then the State Agency should resubmit the verification request a second

time through EVS or SVES. The State Agency may refer the client to the SSA field office for a replacement Social Security card, if necessary.

5. To provide cost-benefit information (e.g., processing costs and program savings) for each program listed in Article II.E. SSA will use this information to justify the efficiencies in the administration of mutually dependent Federal and State programs.

B. SSA agrees:

1. To initially verify the SSNs submitted and to process only verified SSNs in the conduct of the matching program.

2. To the extent permitted by applicable law, to furnish to the State Agency files containing the necessary information for identified individuals via BENDEX or SVES. The files provided by SSA will adhere to the characteristics and data format requirements shown in Attachment B.

3. To the extent permitted by applicable law, to disclose to the State Agency, via BENDEX or SVES, based on its request, Social Security benefit payment and tax return information contained in SSA's records regarding those individuals whom the State Agency identifies. SSA will provide additional information about each individual identified by the State Agency whenever SSA posts changes to its records until the individual dies or the State Agency notifies SSA that the individual is no longer eligible for assistance under the programs identified in Article II.E.

4. To the extent permitted by applicable law, to disclose to the State Agency, via SDX or SVES, payment information contained in SSA's records concerning applicants/recipients of SSI and SVB payments. The files provided by SSA will be IBM compatible and will adhere to the characteristics and information format requirements shown in Attachment B.

5. To the extent permitted by applicable law, to disclose to the State Agency, via EVS or SVES, whether or not the identifying information and SSN furnished agree with SSA records and, if not, what element of information (name, date of birth, or sex code) does not agree. Any multiple SSNs also will be furnished to the State Agency.

XVII. Reimbursement

SSA estimates it will incur approximately $2.3 million in administrative costs to perform matching operations under this national program. This includes expenses for systems' programming and ongoing transaction costs. However, SSA will accrue savings estimated at $24.1 million because manual processes in field offices will be supplanted by automated interfaces. This equates to a 10.5:1 benefit-to-cost ratio for SSA. The State Agencies will

also accrue sizable program savings estimated to be about $3.8 billion. Consequently, the parties recognize the mutual benefits of the matching program and agree to a quid pro quo arrangement in which no cost reimbursement is required. Adjustments may be required in the future if it is determined that costs are disproportionate. Such adjustments, if necessary, will be negotiated and documented in a separate reimbursable agreement.

XVIII. Persons to Contact

A. The SSA contacts are:

1. Data Exchange Agreement Issues:

Norma Followell
Office of Income Security Programs
Information Exchange and Matching Staff
74 RRCC
6401 Security Boulevard
Baltimore, Maryland 21235
Phone: (410) 965-0806
Fax: (410) 597-0841
Email: Norma.Followell@ssa.gov

2. Disclosure Policy Issues

Willie Polk
Office of the General Counsel, Office of Public Disclosure
6401 Security Boulevard
Baltimore, Maryland 21235
Phone: (410) 965-1753
Fax: (410) 966-0869
Email: willie.j.polk@ssa.gov

3. Regional Office:

Alan Follett
Program Expert, Retirement and Survivors Insurance Team
P.O. Box 4206
Richmond, CA 94804
Phone: (510) 970-8245
Fax : (510) 970-8101
Email: Alan.Follett@ssa.gov

4. Systems Issues:

Mark Dailey
Office of Earnings, Enumeration
and Administrative Systems/DIVES/Data Exchange Branch
6401 Security Boulevard
Baltimore, Maryland 21235
Phone: (410) 966-7849
Fax: (410) 966-3147
Email: mark.dailey@ssa.gov

5. Systems Security Issues:

Teresa Rojas, Acting Director
Office of Systems Security Operations Management
Office of Financial Policy and Operations
6401 Security Boulevard
Baltimore, Maryland 21235
Phone: (410) 966-7284
Fax: (410) 966-0527
Email: Teresa.C.Rojas@ssa.gov

B. The State Agency contacts are:

1. Data Exchange Agreement Issues:

John Zapata
Staff Services Manager I, Medi-Cal Eligibility Branch
1501 Capitol Avenue, Suite 71-4331, MS 4607
PO Box 997417
Phone: 916-552-9451
FAX: 916-552-9478
E-Mail: john.zapata@dhcs.ca.gov

2. Systems Security Issues:

Racheal Strider
Chief Information Security Officer
1615 Capitol Avenue, 173.2.233, MS Code 6302
Sacramento, CA 95814
Phone: (916) 440-7223
FAX: (916) 440-7064
E-mail: racheal.strider@dhcs.ca.gov

XIX. Authorized Officials

The State officials with authority to request information under this agreement are the director and her designees.

XX. Agency Approval

Each party executing this Agreement is authorized to enter into agreements of this nature on behalf of their agency.

Social Security Administration:

BY: Nancy Nelson
Associate Commissioner
Office of Income Security Programs

2/12/07
(Date)

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

BY: Manuel J. Vaz
Acting Chairman
Data Integrity Board

3-27-2007
(Date)

XXI. 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. The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement effective this ___day of _____, 2007.

SOCIAL SECURITY ADMINISTRATION:

_____

Peter D. Spencer
San Francisco Regional Commissioner

CALIFORNIA DEPARTMENT OF HEALTH SERVICES
(CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES):

_____

Stan Rosenstein
Deputy Director, Medical Care Services

I, Roberta Ward, certify that I am the legal counsel for the Agency of the State of California; that Stan Rosenstein, who signed this agreement on behalf of the State Agency, was then Deputy Director, Medical Care Services, of said State Agency, and that he is authorized to enter into agreements of this nature on behalf of the State Agency and that there is authority under the laws of the State of California to carry out all the functions to be performed by the State Agency as provided herein and comply with the terms of this agreement.

_____

Roberta Ward
Department of Health Care Services – Privacy Officer and Senior Counsel

Attachment A - Disclosure of Information in Possession of Agency [section 1106 of the Social Security Act (42 U.S.C. § 1306)]
Attachment B - Data elements (in record layout format)
Attachment C - Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration
Attachment D - Worksheet for Reporting Loss or Potential Loss of PII

ATTACHMENT

Information System Security Guidelines For Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration

Social Security Administration
Office of Systems Security Operations Management

Version 3 March 2007

I. Purpose

This document provides security guidelines for Federal, State and Local agencies (hereafter referred to as '**outside entity**') that obtain information electronically from the Social Security Administration (SSA) through information exchange systems. The guidelines are intended to assist SSA's information exchange partners to understand the criteria SSA will use when evaluating and certifying the system design and security features and protocols used for electronic access to SSA information. The guidelines also will be used as the framework for SSA's compliance review program of its information exchange partners.

II. Role of the SSA Office of Systems Security Operations Management

The SSA Office of Systems Security Operations Management (OSSOM) 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 training and awareness materials and providing consultation and support for a variety of agency initiatives. OSSOM reviews assure external systems that receive information from SSA are secure and operate in a manner that is consistent with SSA's IT security policies and are in compliance with the terms of information sharing agreements executed by SSA and the outside entity. Within the context of these guidelines, OSSOM conducts periodic compliance reviews of outside entities that use, maintain, transmit or store SSA data in accordance with pertinent Federal requirements to include the following:

- The Federal Information Security Management Act (FISMA)
- Social Security Administration (SSA) policies, standards, procedures and directives.

Correspondence should be sent to:

Director, Office of Systems Security Operations Management
Social Security Administration
Room G-D-10 East High Rise
6401 Security Blvd.
Baltimore, MD 21235

You can also send an email to OSSOM.admin@ssa.gov.

III. General Systems Security Standards

Outside entities that request and receive information from SSA through online, overnight, or periodic batch transmissions must comply with the following general

systems security standards concerning access to and control of SSA information. The outside entity must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information received from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The outside entity must employ both physical and technological safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

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

IV. Technical and Procedural System Security Requirements

Outside entities that receive SSA information must comply with the following technical and procedural systems security requirements which must be met before SSA will approve a request for access to SSA information. The outside entity's system security design and procedures must conform to these requirements. They must be documented by the outside entity and certified by SSA prior to initiating transactions to and from SSA through batch data exchange processes or online processes such as State On Line Query (SOLQ) or Internet SOLQ.

No specific format for submitting security compliance documentation to SSA is required. However, regardless of how it is presented, the information should be submitted to SSA in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the outside entity with authority to certify the organization's intent to comply with SSA requirements. Written documentation should address each of the following security control areas:

A. General System Security Design and Operating Environment

The outside entity must provide a written description of it's' system configuration and security features. This should include the following:

1. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and

2. A description of how SSA information will be obtained by and presented to users, including sample computer screen presentation formats and an

explanation of whether the system will request information from SSA by means of systems generated or user initiated transactions; and

3. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the outside entity's system and an explanation of their job descriptions.

Meeting this Requirement

Outside entities must explain in their documentation the overall design and security features of their system. During onsite certification and periodic compliance reviews, SSA will use the outside entity's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and compliance reviews and for verifying that the outside entity's systems and procedures conform to SSA requirements.

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

B. Automated Audit Trail

Outside entities that receive information electronically from SSA are required to maintain an automated audit trail record identifying either the individual user, or the system process, that initiated a request for information from SSA. (Every request for information from SSA should be traceable to the individual or system process that initiated the transaction.) Outside entities that request information from SSA only through batch selection processes from their client data bases need only keep audit trail records identifying the process that generated the transactions forwarded to SSA. However, if such processes are triggered as a result of user requests initiated from the entity's client data base, then the audit trail record must be able to identify the user who initiated the transaction. The audit trail system must be capable of data collection, data retrieval and data storage. At a minimum, individual audit trail records must contain the data needed to associate each query transaction to its initiator and relevant business purpose (i.e. the outside entity's client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for

a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before SSA will approve the outside entity's request for access to SSA information.

If SSA-supplied information is retained in the outside entity's system, or if certain data elements within the outside entity's system will indicate to users that the information has been verified by SSA, the outside entity's system also must capture an audit trail record of any user who views SSA information stored within the outside entity's system. The audit trail requirements for these inquiry transactions are the same as those outlined above for the outside entity's transactions requesting information directly from SSA.
Note: Outside entities that receive SSA information through batch processes must maintain an audit trail, but record retrieval may be either manual or automated. For SOLQ/SOLQ-I, the audit trail must be fully automated, including retrieval of individual audit transaction records.

Meeting this Requirement

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

During periodic compliance reviews (see below), the SSA also will test the outside entity's audit trail capability by requesting verification of a sample of transactions it has received from the outside entity after implementation of access to SSA information

C. System Access Control

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

code. The outside entity must have management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the outside entity's system.

Meeting this Requirement

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

During onsite certification and compliance reviews, the SSA will meet with the individual(s) responsible for these functions to verify their responsibilities in the outside entity's access control process and will observe a demonstration of the procedures for logging onto the outside entity's system and accessing SSA information.

D. Monitoring and Anomaly Detection

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

If the outside entity design does not include either of the security control features described above, then the outside entity must develop and implement compensating security controls to prevent their employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of queries requested by individual employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The system must 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 ID's when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password.

- Inquiry match exception reports

  This type of report captures information about users who may be initiating transactions for Social Security Numbers that have no client case association within the outside entity system. **(100% of these cases must be reviewed by 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 information.

- Inquiry activity statistical reports

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

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

Meeting this Requirement

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

explain how the system design will prevent outside entity employees from browsing SSA records.

If the outside entity system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an outside entity client), then the outside entity must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA information. The outside entity should include sample report formats demonstrating their capability to produce the types of reports described above. The outside entity should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification and compliance reviews, the SSA will request a demonstration of the outside entity's monitoring and anomaly detection capability.

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

- If the design is based on a permission module, the outside entity will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the outside entity system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the outside entity system.)

- If the design is based on systematic and/or managerial monitoring and oversight, the outside entity will provide copies of anomaly detection reports and demonstrate the report production capability.

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

E. Management Oversight and Quality Assurance

The outside entity must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information and to ensure there is ongoing

compliance with the terms of the outside entity's data exchange agreement with SSA. The management oversight function must consist of one or more outside entity management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to determine whether the requests comply with these guidelines. These functions should be performed by outside entity employees whose job functions are separate from those who request or use information from SSA.

Meeting this Requirement

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

During onsite certification and compliance reviews, the SSA will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

F. Security Awareness and Employee Sanctions

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

Meeting this Requirement

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

During onsite certification and periodic compliance reviews, the SSA will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The SSA will also meet with a sample of outside entity employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

G. Data and Communications Security

The outside entity will encrypt all SSN and/or SSN-related information when it is transmitted across dedicated communications circuits between its system, or for intrastate communication among it's local office locations. The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

H. SOLQ/SOLQ-I Onsite Systems Security Certification Review

The outside entity must participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the SOLQ/SOLQ-I system. The onsite certification and compliance reviews will address each of the requirements described above and will include, where appropriate, a demonstration of the outside entity's implementation of each requirement. The review will include a walkthrough of the outside entity's data center to observe and document physical security safeguards, a demonstration of the outside entity's implementation of online access to SSA information, and discussions with managers/supervisors. The SSA, or other certifier, also will visit at least one of the outside entity's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.

The SSA will separately document and certify the outside entity's compliance with each SSA security requirement. Any unresolved or unimplemented security control features must be resolved by the outside entity before SSA will authorize their connection to SSA through the SOLQ or SOLQ-I system.

Following a successful security certification review, both parties will sign a document indicating the entity's willingness to comply with these guidelines. Thereafter, the outside entity must participate in a follow-up certification review conducted by SSA after live transmission of online information, and in periodic compliance reviews conducted according to the timeframe established by the information sharing agreement with SSA.

I. Periodic Onsite Compliance Reviews

SSA conducts onsite compliance reviews approximately once every three years, or as needed if there is a significant change in the outside entity's computing platform, or if there is a violation of any of SSA's systems security requirements or an unauthorized disclosure of SSA information by the outside entity. The format of those reviews generally consists of reviewing and updating the outside entity's compliance with the systems security requirements described above.