

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE COUNTY OF ORANGE SOCIAL SERVICES AGENCY
AND
SANTA ANA UNIFIED SCHOOL DISTRICT
FOR THE PROVISION OF
CALWIN EXTRACT FOR MEDI-CAL DIRECT CERTIFICATION

This Memorandum of Understanding (MOU) is entered into by and between the County of Orange, acting through its Social Services Agency, hereinafter referred to as "SSA," and Santa Ana Unified School District, hereinafter referred to as "SAUSD." This MOU contains program content and purpose along with specific guidelines for identifying students to be directly certified for free school meals.

SSA and SAUSD may be referred to individually as "Party" and collectively as "the Parties." The County of Orange may be referred to as "COUNTY." The relationship between SSA and SAUSD, with regard to this MOU, is based upon the following:

1. This MOU is provided for pursuant to the State of California Department of Health Care Services Medi-Cal Eligibility Division Information Letter Number I 15-09 dated March 20, 2015.
2. SAUSD desires to have SSA verify whether individual students meet certain Medi-Cal eligibility criteria defined in this MOU in order to provide free school meals.
3. SSA is willing to verify certain Medi-Cal eligibility criteria under the terms and conditions hereafter set forth.
4. This MOU sets forth the guidelines authorized by both the SSA Director and the SAUSD Deputy Superintendent, Operations for their respective employees to follow in providing services.

TABLE OF CONTENTS

I.	TERM.....	3
II.	PURPOSE.....	3
III.	DEFINITIONS.....	3
IV.	POPULATION TO BE SERVED.....	4
V.	SCOPE OF WORK.....	4
VI.	SYSTEMS AND NETWORK SECURITY.....	4
VII.	COMPLIANCE WITH THE CALIFORNIA DEPARTMENT HEALTH CARE SERVICES MEDI-CAL PRIVACY AND SECURITY AGREEMENT.....	5
VIII.	LICENSES AND STANDARDS.....	5
IX.	CONFIDENTIALITY.....	6
X.	PUBLICITY.....	7
XI.	INDEMNIFICATION.....	8
XII.	INSURANCE.....	8
XIII.	RECORDS.....	11
XIV.	CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING.....	11
XV.	NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW..	12
XVI.	NOTICES.....	12
XVII.	RESOLUTION OF CONFLICTS.....	13
XVIII.	CONFLICT OF INTEREST.....	13
XIX.	TERMINATION.....	14
XX.	GENERAL PROVISIONS.....	14

I. TERM

The term of this MOU shall commence on August 26, 2015, and end on August 31, 2017, unless earlier terminated pursuant to the provisions of Paragraph XIX of this MOU; however, the Parties shall be obligated to perform such duties as would normally extend beyond this term, including but not limited to obligations with respect to indemnification and confidentiality. SSA and SAUSD may mutually agree in writing to extend the term of this MOU for up to twelve (12) additional months upon the same terms and conditions.

II. PURPOSE

The purpose of this MOU is for SAUSD to participate in the U.S. Department of Agriculture's Medicaid Direct Certification Demonstration Project (Project). Participation in the Project may potentially identify more students as low-income for the purpose of becoming directly certified for free school meals.

III. DEFINITIONS

- A. CalWIN: SSA's electronic data system that records Participant activities and progress, payments on behalf of clients, and program eligibility determination.
- B. CWIN ID: Unique identifier or number assigned to each individual in a household or family.
- C. Case ID: Unique identifier or number assigned to each household or family.
- D. Medi-Cal Personally Identifiable Information (PII): PII directly obtained in the course of performing an administrative function on behalf of Medi-Cal 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.

IV. POPULATION TO BE SERVED

The population to be served under this MOU shall be students enrolled in the Santa Ana Unified School District.

V. SCOPE OF WORK

A. No later than the fifth (5th) business day of each month, SAUSD will provide SSA with a list of enrolled students that includes the full name of the students, date of birth, gender, the name of the current school attending and the CalWIN Case ID, CWIN ID or Social Security Number (if known).

B. Students in receipt of Medi-Cal benefits and are members of households with incomes that do not exceed one hundred thirty three percent (133%) of the Federal poverty level for their household size and are not currently participating in any other assistance program will be considered a Project match and confirmed as eligible for Federal meal programs.

C. SSA will review student information provided by SAUSD and certify Medi-Cal covered students by indicating which students are benefit recipients meeting the income criteria in Subparagraph V.B above for the reporting month. SSA will provide the certified list to SAUSD no later than the eighth (8th) business day of each month. The accuracy of the eligibility certification is dependent on SSA's ability to match the data provided by SAUSD with CalWIN data.

VI. SYSTEMS AND NETWORK SECURITY

A. SAUSD warrants that the Partners Data Interchange System (PDIS), utilized as the mechanism for data transfer, provides adequate security and privacy (where "security" is defined as protection of

software and data from natural or human-caused hazards and unauthorized access and manipulation, and “privacy” is defined as protection of personal data from unauthorized access or disclosure), and contains mechanisms to minimize the risk of unauthorized access to shared data. COUNTY hereby acknowledges that fundamental security, privacy and integrity controls are provided by PDIS.

- B. At all times during the term of this MOU, both Parties shall use industry standard information security procedures to protect shared data from inadvertent or unauthorized disclosure or loss.
- C. Any breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII shall be immediately reported to SSA.

VII. COMPLIANCE WITH THE CALIFORNIA DEPARTMENT HEALTH CARE SERVICES MEDI-CAL PRIVACY AND SECURITY AGREEMENT

SAUSD agrees to comply with substantive privacy and security requirements in the Medi-Cal Privacy and Security Agreement between the California Department of Health Care Services (DHCS) and the County of Orange, attached hereto as Exhibit A and incorporated herein.

VIII. LICENSES AND STANDARDS

- A. SAUSD warrants that it has all necessary licenses and permits required by the laws of the United States, State of California, County of Orange and all other appropriate governmental agencies to perform the services described in this Agreement, and agrees to maintain these licenses and permits in effect for the duration of this Agreement. Further, SAUSD warrants that its employees shall conduct themselves in compliance with such laws and licensure requirements including, without limitation, compliance with laws applicable to sexual harassment and ethical behavior.

- B. In the performance of this Agreement, SAUSD shall comply, unless waived in whole or in part by SSA, with all applicable provisions of the California Welfare and Institutions Code (WIC); Title 45 of the Code of Federal Regulations (CFR); Federal Office of Management and Budget (OMB) Circulars A-21, A-122, and A-87; Title 48 CFR Section 31.2; and all applicable laws and regulations of the United States, State of California, County of Orange Social Services Agency and all administrative regulations, rules and policies adopted thereunder as each and all may now exist or be hereafter amended.
- C. Both SSA and SAUSD shall maintain an organizational structure and sufficient staff, within any budgetary constraints, to efficiently and effectively administer and supervise the functions and responsibilities set out in this MOU. Each agency shall ensure staff is conforming to this MOU and applicable State and Federal laws and regulations by supervising, auditing, and reviewing procedures. Revisions will be made as needed to ensure adherence. SSA will ensure that all approved processes and instructions are followed to ensure the requested information is provided to SAUSD.

IX. CONFIDENTIALITY

- A. SSA and SAUSD agree to maintain confidentiality of all records pursuant to WIC Sections 10850-10853, 14100.2, the CDSS MPP, Division 19-000, and all other provisions of law, and regulations promulgated thereunder relating to privacy and confidentiality, as each may now exist or be hereafter amended.
- B. All records and information concerning any and all persons referred to SAUSD by SSA or SSA's designee shall be considered and kept confidential by SAUSD, SAUSD's staff, agents, employees and volunteers. SAUSD shall require all of its employees, agents,

subcontractors and volunteer staff who may provide services for SAUSD under this MOU to sign an agreement with SAUSD before commencing the provision of any such services, to maintain the confidentiality of any and all materials and information with which they may come into contact, or the identities or any identifying characteristics or information with respect to any and all participants referred to SAUSD by SSA, except as may be required to provide services under this MOU or to those specified in this MOU as having the capacity to audit SAUSD, and as to the latter, only during such audit. SAUSD shall provide reports and any other information required by COUNTY in the administration of this MOU, and as otherwise permitted by law.

- C. SAUSD shall inform all of its employees, agents, subcontractors, volunteers and partners of this provision and that any person violating the provisions of said State law may be guilty of a crime.

X. PUBLICITY

- A. SAUSD shall not disclose any details in connection with this MOU to any person or entity except as may be otherwise provided hereunder or required by law.
 - 1. SAUSD shall develop all publicity material in a professional manner; and
 - 2. During the term of this MOU, SAUSD shall not, and shall not authorize another to, publish or disseminate any commercial advertisements, press releases, feature articles, or other materials using the name of COUNTY without the prior written consent of COUNTY. COUNTY shall not unreasonably withhold written consent.

XI. INDEMNIFICATION

SAUSD agrees to indemnify, defend with counsel approved in writing by COUNTY, and hold U.S. Department of Health and Human Services, the State, COUNTY, and their elected and appointed officials, officers, employees, agents and those special districts and agencies which COUNTY's Board of Supervisors acts as the governing Board ('COUNTY INDEMNITEES') harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided by SAUSD pursuant to this MOU. If judgment is entered against SAUSD and COUNTY by a court of competent jurisdiction because of the concurrent active negligence of COUNTY or COUNTY INDEMNITEES, SAUSD and COUNTY agree that liability will be apportioned as determined by the court. Neither Party shall request a jury apportionment.

XII. INSURANCE

- A. Prior to the provision of services under this MOU, SAUSD agrees to purchase all required insurance at SAUSD's expense and to deposit with SSA Certificates of Insurance, including all endorsements required herein, necessary to satisfy COUNTY that the insurance provisions of this MOU have been complied with, and to keep such insurance coverage and the certificates therefore on deposit with SSA during the entire term of this MOU.
- B. All self-insured retentions (SIRs) and deductibles shall be clearly stated on the Certificate of Insurance. If no SIRs or deductibles apply, indicate this on the Certificate of Insurance with a zero (0) by the appropriate line of coverage. Any self-insured retention (SIR) or deductible in an amount in excess of \$25,000 shall specifically be approved by the County Executive

Office (CEO)/Office of Risk Management upon review of SAUSD's current audited financial report.

C. If SAUSD fails to maintain insurance acceptable to COUNTY for the full term of this MOU, COUNTY may terminate this MOU.

D. Qualified Insurer:

1. The policy or policies of insurance required herein must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the Best's Key Rating Guide/Property-Casualty/United States or ambest.com). It is preferred, but not mandatory, that the insurer be licensed to do business in the state of California (California Admitted Carrier).

E. If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial rating.

F. The policy or policies of insurance maintained by SAUSD shall provide the minimum limits and coverage as set forth below:

<u>Coverage</u>	<u>Minimum Limits</u>
Commercial General Liability	\$1,000,000 per occurrence \$2,000,000 aggregate

G. Required Coverage Forms:

Commercial General Liability coverage shall be written on Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability coverage at least as broad.

H. Required Endorsements:

1. Commercial General Liability policy shall contain the following endorsements, which shall accompany the

Certificate of Insurance:

- a. An Additional Insured endorsement using ISO form CG 2010 or CG 2033 or a form at least as broad naming the County of Orange, its elected and appointed officials, officers, employees, agents as Additional Insureds.
 - b. A primary non-contributing endorsement evidencing that CONTRACTOR's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.
- I. All insurance policies required by this MOU shall waive all rights of subrogation against the County of Orange, its elected and appointed officials, officers, agents and employees when acting within the scope of their appointment or employment.
 - J. SAUSD shall notify SSA in writing within thirty (30) days of any policy cancellation and ten (10) days for non-payment of premium and provide a copy of the cancellation notice to SSA. Failure to provide written notice of cancellation may constitute a material breach of the MOU, upon which SSA may suspend or terminate this MOU.
 - K. The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).
 - L. Insurance certificates should be mailed to SSA at the address indicated in Paragraph XVI of this MOU.
 - M. If SAUSD fails to provide the insurance certificates and endorsements within seven (7) days of notification by CEO/County Procurement Office or SSA, COUNTY may terminate this MOU.
 - N. COUNTY expressly retains the right to require SAUSD to increase or decrease insurance of any of the above insurance types throughout

the term of this MOU. Any increase or decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect COUNTY.

- O. COUNTY shall notify SAUSD in writing of changes in the insurance requirements. If SAUSD does not deposit copies of acceptable certificates of insurance and endorsements with COUNTY incorporating such changes within thirty (30) days of receipt of such notice, this MOU may be in breach without further notice to SAUSD, and COUNTY shall be entitled to all legal remedies.
- P. The procuring of such required policy or policies of insurance shall not be construed to limit SAUSD's liability hereunder nor to fulfill the indemnification provisions and requirements of this MOU, nor act in any way to reduce the policy coverage and limits available from the insurer.

XIII. RECORDS

With the exception of any client records or other records referenced in Paragraph VI, entitled Confidentiality, all records, including but not limited to, reports, audits, notices, claims, statements and correspondence, required by this MOU may be subject to public disclosure. COUNTY will not be liable for any such disclosure.

XIV. CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING

SAUSD shall establish a procedure acceptable to SSA to ensure that all employees, volunteers, consultants, or agents performing services under this MOU report child abuse or neglect to one of the agencies specified in Penal Code Section 11165.9 and dependent adult or elder abuse as defined in Section 15610.07 of the WIC to one of the agencies specified in WIC Section 15630. SAUSD shall require such employee, volunteer, consultant or agent to sign a statement acknowledging the child abuse reporting requirements set forth in Sections 11166 and 11166.05 of the

Penal Code and the dependent adult and elder abuse reporting requirements as set forth in Section 15630 of the WIC and will comply with the provisions of these code sections as they now exist or as they may hereafter be amended.

XV. NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW

SAUSD shall notify and provide to its employees, a fact sheet regarding the Safely Surrendered Baby Law, its implementation in Orange County, and where and how to safely surrender a baby. The fact sheet is available on the Internet at www.babysafe.ca.gov for printing purposes. The information shall be posted in all reception areas where clients are served.

XVI. NOTICES

All notices, claims correspondence, reports, and/or statements authorized or required by this MOU shall be addressed as follows:

SSA: County of Orange Social Services Agency
Contract Services
500 N. State College Blvd.
Orange, CA 92868

SAUSD: Santa Ana Unified School District
Stefanie P. Phillips, Ed.D., Deputy Superintendent,
Operations 714-558-5826
Mark Chavez, Director of Nutrition Services 714-431-1900
1601 East Chestnut Ave.
Santa Ana, CA 92701

All notices shall be deemed effective when in writing and deposited in the United States mail, first class, postage prepaid and addressed as above. Any notices, claims, correspondence, reports and/or statements authorized or required by this MOU addressed in any other fashion shall be deemed not given. SSA and SAUSD may mutually agree in writing to

change the addresses, phone numbers and names of individuals to which notices are sent.

XVII. RESOLUTION OF CONFLICTS

For resolution of conflicts between SSA and SAUSD in regards to the provisions of this MOU, the following may be used:

- Step 1: Conference between the SSA Medi-Cal Program Administrative Manager I and the SAUSD Director of Nutrition Services.
- Step 2: Conference between the SSA Medi-Cal Program Administrative Manager II and the SAUSD Assistant Superintendent of Business Services.
- Step 3: Conference between the SSA Deputy Director of Adult Services and Assistance Program, or designee, and the SAUSD Deputy Superintendent, Operations.

Nothing in this Paragraph limits the rights of the Parties under Paragraph XIX.

XVIII. CONFLICT OF INTEREST

- A. SAUSD shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of COUNTY. This obligation shall apply to SAUSD's employees, agents, relatives, and third parties associated with accomplishing the work hereunder.
- B. SAUSD's efforts shall include, but not be limited to, establishing precautions to prevent its employees or agents from making, receiving, providing, or offering gifts, entertainment, payments, loans, or other considerations which could be deemed to appear to influence individuals to act contrary to the best interests of COUNTY.

XIX. TERMINATION

- A. SSA may terminate this MOU without penalty immediately with cause or after thirty (30) days' written notice without cause, unless otherwise specified. Notice shall be deemed served on the date of mailing. Cause shall be defined as any breach of this MOU, any misrepresentation, or fraud on the part of SAUSD. Exercise by SSA of the right to terminate this MOU shall relieve COUNTY of all further obligations under this MOU.
- B. Upon termination, or notice thereof, SAUSD agree to cooperate with SSA in the orderly transfer of service responsibilities, active case records, and pertinent documents.
- C. The obligations of SSA under this MOU are contingent upon the availability of Federal and/or State funds, as applicable, and inclusion of sufficient funds for the services hereunder in the budget approved by the Orange County Board of Supervisors each fiscal year this MOU remains in effect or operation. In the event that such funding is terminated or reduced, SSA may immediately terminate or modify this MOU, without penalty. The decision of SSA shall be binding on SAUSD. SSA shall provide SAUSD with written notification of such determination. SAUSD shall immediately comply with SSA's decision.

XX. GENERAL PROVISIONS

- A. Nothing herein contained shall be construed as creating the relationship of employer and employee, or principal and agent, between SSA and any participant participating in this program, or any of SAUSD's agents or employees.
- B. This MOU represents the entire understanding of the Parties with respect to the subject matter. No change, modification, extension, termination or waiver of this MOU, or any of the

understandings herein contained, shall be valid unless made in writing and signed by duly authorized representatives of the Parties hereto.

- C. This MOU has been negotiated and executed in the State of California and shall be governed by and construed under the laws of the State of California. In the event of any legal action to enforce or interpret this MOU, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the Parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure Section 394. Furthermore, the Parties specifically agree to waive any and all rights to request that an action be transferred for trial to another county.
- D. The Parties agree that separate copies of this MOU may be signed by each of the Parties, and this MOU will have the same force and effect as if the original had been signed by all the Parties.
- E. If any provision of this MOU or the application thereof is held invalid, the remainder of this MOU shall not be affected thereby.

WHEREFORE, the Parties hereto have executed the Memorandum of Understanding in the County of Orange.

By: _____

Michael F. Ryan, Director
County of Orange
Social Services Agency

Dated: _____

By: _____

Stefanie P. Phillips, Ed.D.,
Deputy Superintendent, Operations
Santa Ana Unified School District

Dated: _____

Approved As To Form
County Counsel
County of Orange, California

By: Annueloo _____

Deputy

Dated: 7/15/15 _____

EXHIBIT A
TO
MEMORANDUM OF UNDERSTANDING
BETWEEN
THE COUNTY OF ORANGE SOCIAL SERVICES AGENCY
AND
SANTA ANA UNIFIED SCHOOL DISTRICT
FOR THE PROVISION OF
CALWIN EXTRACT FOR MEDI-CAL DIRECT CERTIFICATION

**MEDI-CAL PRIVACY AND SECURITY AGREEMENT BETWEEN
the California Department of Health Care Services and the
County of _____, Department of _____**

PREAMBLE

The Department of Health Care Services (DHCS) and the County of _____, Department of _____ (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 California’s Medicaid Program (Medi-Cal). The County Department assists in the administration of Medi-Cal, in that DHCS and the County Department access DHCS eligibility information for the purpose of determining Medi-Cal eligibility.

This Agreement covers the County of _____, Department of _____ workers, who assist in the administration of Medi-Cal; and access, use, or disclose Medi-Cal PII.

DEFINITIONS

For the purpose of this Agreement, the following terms mean:

1. “Assist in the administration of the Medi-Cal program” means performing administrative functions on behalf of Medi-Cal, such as determining eligibility for, or enrollment in, or the amount of, public benefits, and collecting Medi-Cal PII for such purposes, to the extent such activities are authorized by law.
2. “Breach” refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to Medi-Cal PII, whether physical, electronic, or in spoken word or recording.
3. “County Worker” means those county employees, contractors, subcontractors, vendors and agents performing job functions for the County that require access to and/or use of Medi-Cal PII and that are authorized by the County to access and use Medi-Cal PII.

4. "Medi-Cal PII" is information directly obtained in the course of performing an administrative function on behalf of Medi-Cal 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.
5. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Medi-Cal PII, or interference with system operations in an information system which processes Medi-Cal PII that is under the control of the County or County's SAWS Consortium, or a contractor, subcontractor or vendor of the County.

AGREEMENTS

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

I. PRIVACY AND CONFIDENTIALITY

- A. The County Department workers covered by this Agreement (County Workers) may use or disclose Medi-Cal PII only as permitted in this Agreement and only to assist in the administration of Medi-Cal 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. Disclosures, which are required by law, such as a court order, or 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. Pursuant to this Agreement, County Workers may use Medi-Cal PII only to perform administrative functions related to determining eligibility for individuals applying for Medi-Cal.
- C. Access to Medi-Cal PII shall be restricted to only County Workers, who need the Medi-Cal PII to perform their official duties to assist in the administration of Medi-Cal.
- D. 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. PERSONNEL CONTROLS

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. ***Employee Training.*** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers, who assist in the administration of Medi-Cal and use or disclose Medi-Cal PII, including;
 1. Provide privacy and security awareness training to each new County Worker within 30 days of employment and thereafter, provide ongoing refresher training or reminders of the privacy and security safeguards in this

Agreement to all County Workers, who assist in the administration of Medi-Cal and use or disclose Medi-Cal PII at least annually;

2. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed;
 3. Retain the most recent training records for a period of three years after completion of the training.
- B. **Employee Discipline.** Apply appropriate sanctions against workforce members, who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. **Confidentiality Statement.** Ensure that all County Workers, who assist in the administration of Medi-Cal, 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 County Workers prior to accessing Medi-Cal PII and the most recent version shall be retained for a period of three years.
- D. **Background Check.** Conduct a background screening of a County Worker before a County Worker may access DHCS PII. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees, who are authorized to bypass significant technical and operational security controls. The County Department shall retain each County Worker's most recent background check documentation for a period of three years.

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 ongoing management oversight including periodic self-assessments and random sampling of work activity by County Workers, who assist in the administration of Medi-Cal and use or disclose Medi-Cal PII. DHCS shall provide the County Department with information on the Medi-Cal Eligibility Data System (MEDS) usage anomalies for investigation and follow-up.
- C. Ensure 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. **INFORMATION SECURITY AND PRIVACY STAFFING**

The County agrees to:

- A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this agreement.

- B. Assign county workers to be responsible for administration and monitoring of all security related controls stated in this Agreement.

V. PHYSICAL SECURITY

The County Department shall ensure 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 the County Department facilities where County Workers assist in the administration of Medi-Cal and use or disclose Medi-Cal PII. The County Department shall ensure these secured 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. Issue County Workers, who assist in the administration of Medi-Cal identification badges and require County Workers to wear these badges at the County Department facilities where Medi-Cal PII is stored or used.
- C. Ensure each physical location, where Medi-Cal PII is used or stored, has procedures and controls that ensure an individual, who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.
- D. Ensure there are security guards or a monitored alarm system with or without security cameras 24 hours a day, seven days a week at the County Department facilities and leased facilities where a large volume of Medi- Cal PII is stored.
- E. Ensure data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of Medi-Cal PII have perimeter security and access controls that limit access to only authorized Information Technology (IT) staff. Visitors to the data center area must be escorted by authorized IT staff at all times.
- F. 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 that indicate 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.
- G. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing Medi-Cal PII.

VI. TECHNICAL SECURITY CONTROLS

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

- C. **Minimum Necessary.** Only the minimum necessary amount of Medi-Cal PII required to perform necessary business functions may be copied, downloaded, or exported.
- D. **Removable media devices.** All electronic files, which contain Medi-Cal PII data, must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128bit or higher, such as AES.
- E. **Antivirus software.** All workstations, laptops and other systems, which process and/or store Medi-Cal PII, must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- F. **Patch Management.** All workstations, laptops and other systems, which process and/or store Medi-Cal PII, must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches deemed as high risk must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.
- G. **User IDs and Password Controls.** All users must be issued a unique user name for accessing Medi-Cal PII. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
- Upper case letters (A-Z)
 - Lower case letters (a-z)
 - Arabic numerals (0-9)
 - Non-alphanumeric characters (punctuation symbols)
- H. **User Access.** Exercise management control and oversight, in conjunction with DHCS, of the function of authorizing individual user access to Social Security Administration (SSA) data, MEDS, and over the process of issuing and maintaining access control numbers and passwords.
- I. **Data Destruction.** When no longer needed, all Medi-Cal PII must be wiped using the Gutmann or U.S. Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88.
- J. **System Timeout.** The system providing access to Medi-Cal PII must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

- K. **Warning Banners.** All systems providing access to Medi-Cal PII must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- L. **System Logging.** The system must maintain an automated audit trail that can identify the user or system process, initiates a request for Medi-Cal PII, or alters Medi-Cal PII. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Medi-Cal PII is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence.
- M. **Access Controls.** The system providing access to Medi-Cal PII must use role based access controls for all user authentications, enforcing the principle of least privilege.
- N. **Transmission encryption.** All data transmissions of Medi-Cal PII outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm that is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing Medi-Cal PII can be encrypted. This requirement pertains to any type of Medi-Cal PII in motion such as website access, file transfer, and E-Mail.
- O. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting Medi-Cal PII, which are accessible through the Internet, must be protected by a comprehensive intrusion detection and prevention solution.

VII. AUDIT CONTROLS

- A. **System Security Review.** The County Department must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Medi-Cal PII must have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate levels of protection. Reviews should include vulnerability scanning tools.
- B. **Log Reviews.** All systems processing and/or storing Medi-Cal PII must have a routine procedure in place to review system logs for unauthorized access.
- C. **Change Control.** All systems processing and/or storing Medi-Cal PII must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.
- D. **Anomalies.** Investigate anomalies in MEDS usage identified by DHCS and report conclusions of such investigations and remediation to DHCS.

VIII. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

- A. **Emergency Mode Operation Plan.** The County Department must establish a documented plan to enable continuation of critical business processes and protection of the security of Medi-Cal PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.
- B. **Data Centers.** Data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of Medi-Cal PII, must

include sufficient environmental protection such as cooling, power, and fire prevention, detection, and suppression.

- C. **Data Backup Plan.** The County Department must have established documented procedures to backup Medi-Cal PII to maintain retrievable exact copies of Medi-Cal PII. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore Medi-Cal PII should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of Medi-Cal data.

IX. PAPER DOCUMENT CONTROLS

- A. **Supervision of Data.** Medi-Cal PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Medi-Cal PII in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. **Escorting Visitors.** Visitors to areas where Medi-Cal PII is contained shall be escorted and Medi-Cal PII shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** Medi-Cal PII must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. **Removal of Data.** Medi-Cal PII must not be removed from the premises of County Department except for identified routine business purposes or with express written permission of DHCS.
- E. **Faxing.** Faxes containing Medi-Cal PII shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.
- F. **Mailing.** Mailings containing Medi-Cal PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible. Mailings that include 500 or more individually identifiable records containing Medi-Cal PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.

X. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this PSA, the County Department agrees to implement reasonable systems for the discovery and prompt reporting of any Breach or Security Incident, and to take the following steps:

- A. **Initial Notice to DHCS.** (1) To notify DHCS **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured Medi-Cal PII in electronic media or in any other media if the PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to DHCS by the SSA. (2) To notify DHCS **within 24 hours by email or fax** of the discovery of any breach, security incident, intrusion, or unauthorized access,

use, or disclosure of Medi-Cal PII in violation of this Agreement, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by the County Department as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the County Department. Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PII, notice shall be provided by calling the DHCS ITSD Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. The County Department shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "County Use" near the middle of the page) or use this link:

<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx>

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII, the County Department shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
 2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- B. **Investigation and Investigative Report.** To immediately investigate a breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII, within 72 hours of the discovery, the County Department shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer.
- C. **Complete Report.** To provide a complete report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten working days of the discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure. The report shall be submitted on the "DHCS Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, County Department shall make reasonable efforts to provide DHCS with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "DHCS Privacy Incident Report" form. DHCS will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.
- D. **Notification of Individuals.** When applicable state or federal law requires DHCS to notify individuals of a breach or unauthorized disclosure of their Medi-

Cal PII, the following provisions apply: If the cause of the breach is attributable to the County Department or its subcontractors, agents or vendors, the County Department shall pay any costs of such notifications, as well as any and all costs associated with the breach. The notifications shall comply with the requirements set forth in California Civil Code Section 1798.29, and 42 U.S.C. section 17932, and its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before notifications are made. DHCS may elect to assign responsibility for such notification to the County Department. In the event DHCS assigns notification responsibility to the County Department, DHCS shall provide the County Department with the appropriate direction and procedures to ensure notice is provided pursuant to applicable law. If the cause of the breach is attributable to DHCS, DHCS shall pay any costs associated with such notifications. If there is any question as to whether DHCS or the County Department is responsible for the breach, DHCS and the County Department shall jointly determine responsibility for purposes of allocating the costs of such notices.

- E. ***Responsibility for Reporting of Breaches when Required by State or Federal Law.*** If the cause of a breach of Medi-Cal PII is attributable to the County Department or its agents, subcontractors or vendors, the County Department is responsible for reporting the breach and all costs associated with the breach. If the cause of the breach is attributable to DHCS, DHCS is responsible for reporting the breach and for all costs associated with the breach. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, DHCS and the County Department shall coordinate to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.
- F. ***DHCS Contact Information.*** To direct communications to the above referenced DHCS staff, the County Department shall initiate contact as indicated herein. DHCS reserves the right to make changes to the contact information below by giving written notice to the County Department. Said changes shall not require an amendment to this Agreement to which it is incorporated.

DHCS Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
Program Integrity and Security Unit Policy Operations Branch Medi-Cal Eligibility Division 1501 Capitol Avenue, MS 4607 P.O. Box 997417 Sacramento, CA 95899-7417 Telephone: (916) 552-9200	Privacy Officer c/o: Office of HIPAA Compliance DHCS Privacy Office, MS 4722 P.O. Box 997413 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office, MS 6400 P.O. Box 997413 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Fax: (916) 440-5537 Telephone: ITSD Service Desk (916) 440-7000 or (800) 579-0874

XI. COMPLIANCE WITH SSA AGREEMENT

The County Department agrees to comply with substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between SSA and DHCS, known as the Information Exchange Agreement (IEA), which are appended and hereby incorporated in to this Agreement (Exhibit A). The specific sections of the IEA with substantive privacy and security requirements, which are to be complied with by the County Department are in the following sections: E, Security Procedures; F, Contractor/Agent Responsibilities; G, Safeguarding and Reporting Responsibilities for PII, and in Attachment 4, Electronic Information Exchange Security Requirements, Guidelines, and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with SSA. If there is any conflict between a privacy and security standard in these sections of the IEA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to Medi-Cal PII.

XII. COUNTY DEPARTMENT'S AGENTS AND SUBCONTRACTORS

The County Department agrees to enter into written agreements with any agents, including subcontractors and vendors, to whom County Department provides Medi-Cal PII received from or created or received by County Department in performing functions or activities related to the administration of Medi-Cal that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to the County Department with respect to Medi-Cal PII, including restrictions on disclosure of Medi-Cal PII and the use of appropriate administrative, physical, and technical safeguards to protect such Medi-Cal PII. The County Department shall incorporate, when applicable, the relevant provisions of this PSA into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII be reported to the County Department.

XIII. 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. 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 DHCS 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.

XIV. 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 County Workers assisting in the administration of Medi-Cal 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 the County Department at no cost to the 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.

XV. AMENDMENT OF AGREEMENT

DHCS and the County Department acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that amendment of this PSA may be required to provide for procedures to ensure compliance with such developments. Upon request by DHCS, the County Department agrees to promptly enter into negotiations concerning an amendment to this PSA as may be needed by developments in federal and state laws and regulations. DHCS may terminate this PSA upon thirty (30) days written notice if the County Department does not promptly enter into negotiations to amend this PSA when requested to do so, or does not enter into an amendment that DHCS deems necessary.

XVI. TERMINATION

This PSA shall terminate three years after the date it is executed, unless the parties agree in writing to extend its term. All provisions of this PSA that provide restrictions on disclosures of Medi-Cal PII and that provide administrative, technical, and physical safeguards for the Medi-Cal PII in the County Department's possession shall continue in effect beyond the termination of the PSA, and shall continue until the Medi-Cal PII is destroyed or returned to DHCS.

XVII. TERMINATION FOR CAUSE

Upon DHCS' knowledge of a material breach or violation of this Agreement by the County Department, DHCS may provide an opportunity for the County Department to cure the breach or end the violation and may terminate this Agreement if the County Department does not cure the breach or end the violation within the time specified by DHCS. This Agreement may be terminated immediately by DHCS if the County Department has breached a material term and DHCS determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, the County Department must destroy all PII in accordance with Section VI.I, above. The provisions of this Agreement governing the privacy and security of the PII shall remain in effect until all PII is destroyed and DHCS receives a certificate of destruction.

XVIII. 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. The contract is effective on the day the final signature is obtained.

For the County of Orange Department of Social Services,
8/20/13

(Signature) (Date)
Dr. Michael Riley Director

(Name) (Title)

For the Department of Health Care Services,

(Signature) (Date)

Toby Douglas Director

(Name) (Title)

Exhibit A: Agreement between SSA and CHHS, and Agreement between SSA and DHCS with Attachment "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the SSA." These are sensitive documents that are provided separately to the County's privacy and security office.